Reference Manual for the ProSafe VPN Firewall FVS318v3

NETGEAR

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA

202-10059-02
Version 3
January 2005

© 2005 by NETGEAR, Inc. All rights reserved.

Trademarks

NETGEAR is a trademark of Netgear, Inc.

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Other brand and product names are registered trademarks or trademarks of their respective holders.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice.

NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

EN 55 022 Declaration of Conformance

This is to certify that the FVS318v3 ProSafe VPN Firewall is shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022 Class B (CISPR 22).

Bestätigung des Herstellers/Importeurs

Es wird hiermit bestätigt, daß das FVS318v3 ProSafe VPN Firewall gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

Das Bundesamt für Zulassungen in der Telekommunikation wurde davon unterrichtet, daß dieses Gerät auf den Markt gebracht wurde und es ist berechtigt, die Serie auf die Erfüllung der Vorschriften hin zu überprüfen.

Certificate of the Manufacturer/Importer

It is hereby certified that the FVS318v3 ProSafe VPN Firewall has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the second category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas.

When used near a radio or TV receiver, it may become the cause of radio interference.

Read instructions for correct handling.

Product and Publication Details

Model Number:	FVS318v3
Publication Date:	January 2005
Product Family:	Router
Product Name:	FVS318v3 ProSafe VPN Firewall
Home or Business Product:	Business
Language:	English

Contents

Chapter 1
About This Manual

Audience, Scope, Conventions, and Formats 1-1
How to Use This Manual 1-2
How to Print this Manual 1-3

Chapter 2
Introduction

Key Features of the VPN Firewall 2-1
A Powerful, True Firewall with Content Filtering 2-2
Security 2-2
Autosensing Ethernet Connections with Auto Uplink 2-3
Extensive Protocol Support 2-3
Easy Installation and Management 2-4
Maintenance and Support 2-4
Package Contents 2-5
The FVS318v3 Front Panel 2-5
The FVS318v3 Rear Panel 2-6
NETGEAR-Related Products 2-7
NETGEAR Product Registration, Support, and Documentation 2-7

Chapter 3
Connecting the Firewall to the Internet

Prepare to Install Your FVS318v3 ProSafe VPN Firewall 3-1
First, Connect the FVS318v3 3-1
Now, Configure the FVS318v3 for Internet Access 3-4
Troubleshooting Tips 3-6
Overview of How to Access the FVS318v3 VPN Firewall 3-8
How to Log On to the FVS318v3 After Configuration Settings Have Been Applied 3-9
How to Bypass the Configuration Assistant 3-10

Using the Smart Setup Wizard 3-11
How to Manually Configure Your Internet Connection 3-12

Chapter 4
Firewall Protection and
Content Filtering

Firewall Protection and Content Filtering Overview 4-1
Block Sites 4-2
Using Rules to Block or Allow Specific Kinds of Traffic 4-3
Inbound Rules (Port Forwarding) 4-5
Inbound Rule Example: A Local Public Web Server 4-5
Inbound Rule Example: Allowing a Videoconference from Restricted Addresses 4-6
Considerations for Inbound Rules 4-6
Outbound Rules (Service Blocking) 4-7
Outbound Rule Example: Blocking Instant Messenger 4-7
Order of Precedence for Rules 4-8
Default DMZ Server 4-8
Respond to Ping on Internet WAN Port 4-9
Services 4-10
Using a Schedule to Block or Allow Specific Traffic 4-12
Time Zone 4-13
Getting E-Mail Notifications of Event Logs and Alerts 4-14
Viewing Logs of Web Access or Attempted Web Access 4-16
Syslog 4-17

Chapter 5
Basic Virtual Private Networking

Overview of VPN Configuration 5-2
Client-to-Gateway VPN Tunnels 5-2
Gateway-to-Gateway VPN Tunnels 5-2
Planning a VPN 5-3
VPN Tunnel Configuration 5-5
How to Set Up a Client-to-Gateway VPN Configuration 5-5
Step 1: Configuring the Client-to-Gateway VPN Tunnel on the FVS318v3 5-6
Step 2: Configuring the NETGEAR ProSafe VPN Client on the Remote PC 5-9
Monitoring the Progress and Status of the VPN Client Connection 5-16
Transferring a Security Policy to Another Client 5-18
Exporting a Security Policy 5-18

Importing a Security Policy 5-19
How to Set Up a Gateway-to-Gateway VPN Configuration 5-20
Procedure to Configure a Gateway-to-Gateway VPN Tunnel 5-21
VPN Tunnel Control 5-26
Activating a VPN Tunnel 5-26
Start Using a VPN Tunnel to Activate It 5-26
Using the VPN Status Page to Activate a VPN Tunnel 5-26
Activate the VPN Tunnel by Pinging the Remote Endpoint 5-27
Verifying the Status of a VPN Tunnel 5-29
Deactivating a VPN Tunnel 5-30
Using the Policy Table on the VPN Policies Page to Deactivate a VPN Tunnel 5-30
Using the VPN Status Page to Deactivate a VPN Tunnel 5-31
Deleting a VPN Tunnel 5-32

Chapter 6
Advanced Virtual Private Networking

Overview of FVS318v3 Policy-Based VPN Configuration 6-1
Using Policies to Manage VPN Traffic 6-2
Using Automatic Key Management 6-2
IKE Policies' Automatic Key and Authentication Management 6-3
VPN Policy Configuration for Auto Key Negotiation 6-5
VPN Policy Configuration for Manual Key Exchange 6-9
Using Digital Certificates for IKE Auto-Policy Authentication 6-13
Certificate Revocation List (CRL) 6-14
Walk-Through of Configuration Scenarios on the FVS318v3 6-14
VPN Consortium Scenario 1:
Gateway-to-Gateway with Preshared Secrets 6-15
FVS318v3 Scenario 1: FVS318v3 to Gateway B IKE and VPN Policies 6-16
How to Check VPN Connections 6-21
Testing the Gateway A FVS318v3 LAN and the Gateway B LAN 6-21
FVS318v3 Scenario 2: FVS318v3 to FVS318v3 with RSA Certificates 6-22

Chapter 7
Maintenance

Viewing VPN Firewall Status Information 7-1
Viewing a List of Attached Devices 7-5
Upgrading the Firewall Software 7-5
Configuration File Management 7-7

Backing Up the Configuration 7-7
Restoring the Configuration 7-7
Erasing the Configuration 7-8
Changing the Administrator Password 7-8

Chapter 8
Advanced Configuration

How to Configure Dynamic DNS 8-1
Using the LAN IP Setup Options 8-2
Configuring LAN TCP/IP Setup Parameters 8-3
Using the Firewall as a DHCP server 8-4
Using Address Reservation 8-5
Configuring Static Routes 8-5
Static Route Example 8-7
Enabling Remote Management Access 8-7

Chapter 9
Troubleshooting

Basic Functioning 9-1
Power LED Not On 9-1
LEDs Never Turn Off 9-2
LAN or Internet Port LEDs Not On 9-2
Troubleshooting the Web Configuration Interface 9-3
Troubleshooting the ISP Connection 9-4
Troubleshooting a TCP/IP Network Using a Ping Utility 9-5
Testing the LAN Path to Your Firewall 9-5
Testing the Path from Your PC to a Remote Device 9-6
Restoring the Default Configuration and Password 9-7
Problems with Date and Time 9-7

Appendix A
Technical Specifications

Appendix B
Network, Routing, and Firewall Basics

Related Publications B-1
Basic Router Concepts B-1
What is a Router? B-2
Routing Information Protocol B-2
IP Addresses and the Internet B-2

Netmask B-4
Subnet Addressing B-5
Private IP Addresses B-7
Single IP Address Operation Using NAT B-8
MAC Addresses and Address Resolution Protocol B-9
Related Documents B-9
Domain Name Server B-9
IP Configuration by DHCP B-10
Internet Security and Firewalls B-10
What is a Firewall? B-11
Stateful Packet Inspection B-11
Denial of Service Attack B-11
Ethernet Cabling B-11
Category 5 Cable Quality B-12
Inside Twisted Pair Cables B-13
Uplink Switches, Crossover Cables, and MDI/MDIX Switching B-14

Appendix C
Virtual Private Networking

What is a VPN? C-1
What Is IPSec and How Does It Work? C-2
IPSec Security Features C-2
IPSec Components C-2
Encapsulating Security Payload (ESP) C-3
Authentication Header (AH) C-4
IKE Security Association C-4
Mode C-5
Key Management C-6
Understand the Process Before You Begin C-6
VPN Process Overview C-7
Network Interfaces and Addresses C-7
Interface Addressing C-7
Firewalls C-8
VPN Tunnel Between Gateways C-8
VPNC IKE Security Parameters C-10
VPNC IKE Phase I Parameters C-10

VPNC IKE Phase II Parameters C-11
Testing and Troubleshooting C-11
Additional Reading C-11

Appendix D
Preparing Your Network

Preparing Your Computers for TCP/IP Networking D-1
Configuring Windows 95, 98, and Me for TCP/IP Networking D-2
Install or Verify Windows Networking Components D-2
Enabling DHCP to Automatically Configure TCP/IP Settings D-4
Selecting Windows' Internet Access Method D-6
Verifying TCP/IP Properties D-6
Configuring Windows NT4, 2000 or XP for IP Networking D-7
Install or Verify Windows Networking Components D-7
Enabling DHCP to Automatically Configure TCP/IP Settings D-8
DHCP Configuration of TCP/IP in Windows XP D-8
DHCP Configuration of TCP/IP in Windows 2000 ..... D-10
DHCP Configuration of TCP/IP in Windows NT4 ..... D-13
Verifying TCP/IP Properties for Windows XP, 2000, and NT4 ..... D-15
Configuring the Macintosh for TCP/IP Networking D-16
MacOS 8.6 or 9.x D-16
MacOS X D-16
Verifying TCP/IP Properties for Macintosh Computers D-17
Verifying the Readiness of Your Internet Account D-18
Are Login Protocols Used? D-18
What Is Your Configuration Information? D-18
Obtaining ISP Configuration Information for Windows Computers D-19
Obtaining ISP Configuration Information for Macintosh Computers D-20
Restarting the Network D-21

Appendix E
VPN Configuration of NETGEAR FVS318v3

Case Study Overview E-1
Gathering the Network Information E-1
Configuring the Gateways E-2
Activating the VPN Tunnel E-5
The FVS318v3-to-FVS318v3 Case E-6

Configuring the VPN Tunnel E-6
Viewing and Editing the VPN Parameters E-9
Initiating and Checking the VPN Connections E-11
The FVS318v3-to-FVS318v2 Case E-13
Configuring the VPN Tunnel E-13
Viewing and Editing the VPN Parameters E-16
Initiating and Checking the VPN Connections E-18
The FVS318v3-to-FVL328 Case E-20
Configuring the VPN Tunnel E-20
Viewing and Editing the VPN Parameters E-23
Initiating and Checking the VPN Connections E-25
The FVS318v3-to-VPN Client Case E-27
Client-to-Gateway VPN Tunnel Overview E-27
Configuring the VPN Tunnel E-28
Initiating and Checking the VPN Connections E-36

Glossary

List of Glossary Terms G-1
Numeric G-1
A G-1
B G-2
C G-2
D G-3
E G-4
G G-4
I G-4
L G-6
M G-6
P G-7
Q G-8
R G-8
S G-9
T G-9
U G-9
W G-9

Chapter 1
About This Manual

This chapter describes the intended audience, scope, conventions, and formats of this manual.

Audience, Scope, Conventions, and Formats

This reference manual assumes that the reader has basic to intermediate computer and Internet skills. However, basic computer network, Internet, firewall, and VPN technologies tutorial information is provided in the Appendices and on the NETGEAR Web site.

This guide uses the following typographical conventions:

Table 1-1. Typographical Conventions

italics	Emphasis, books, CDs, URL names
bold	User input
`fixed`	Screen text, file and server names, extensions, commands, IP addresses

This guide uses the following formats to highlight special messages:

Note: This format is used to highlight information of importance or special interest.

This manual is written for the FVS318v3 VPN Firewall according to these specifications.:

Table 1-2. Manual Scope

Product Version	FVS318v3 ProSafe VPN Firewall
Manual Publication Date	January 2005

Note: Product updates are available on the NETGEAR, Inc. Web site at *http://kbserver.netgear.com/products/FVS318v3.asp*.

How to Use This Manual

The HTML version of this manual includes the following:

- Buttons, > and <, for browsing forwards or backwards through the manual one page at a time
- A TOC button that displays the table of contents and an Index button. Double-click on a link in the table of contents or index to navigate directly to where the topic is described in the manual.
- A Knowledge Base button to access the full NETGEAR, Inc. online Knowledge Base for the product model.
- Links to PDF versions of the full manual and individual chapters.

How to Print this Manual

To print this manual you can choose one of the following several options, according to your needs.

- **Printing a Page in the HTML View**.

  Each page in the HTML version of the manual is dedicated to a major topic. Use the *Print* button on the browser toolbar to print the page contents.

- **Printing a Chapter**.

  Use the *PDF of This Chapter* link at the top left of any page.

  – Click the "*PDF of This Chapter*" link at the top right of any page in the chapter you want to print. The PDF version of the chapter you were viewing opens in a browser window.

    Note: Your computer must have the free Adobe Acrobat reader installed in order to view and print PDF files. The Acrobat reader is available on the Adobe Web site at *http://www.adobe.com*.

  – Click the print icon in the upper left of the window.

    Tip: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

- **Printing the Full Manual**.

  Use the *Complete PDF Manual* link at the top left of any page.

  – Click the *Complete PDF Manual* link at the top left of any page in the manual. The PDF version of the complete manual opens in a browser window.
  – Click the print icon in the upper left of the window.

    Tip: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

Chapter 2
Introduction

This chapter describes the features of the NETGEAR FVS318v3 ProSafe VPN Firewall.

Key Features of the VPN Firewall

The FVS318v3 ProSafe VPN Firewall with eight-port switch connects your local area network (LAN) to the Internet through an external access device such as a cable modem or DSL modem.

The FVS318v3 is a complete security solution that protects your network from attacks and intrusions. Unlike simple Internet sharing firewalls that rely on Network Address Translation (NAT) for security, the FVS318v3 uses stateful packet inspection for Denial of Service attack (DoS) protection and intrusion detection. The FVS318v3 allows Internet access for up to 253 users. The FVS318v3 VPN Firewall provides you with multiple Web content filtering options, plus browsing activity reporting and instant alerts — both via e-mail. Parents and network administrators can establish restricted access policies based on time-of-day, Web site addresses and address keywords, and share high-speed cable/DSL Internet access for up to 253 personal computers. In addition to NAT, the built-in firewall protects you from hackers.

With minimum setup, you can install and use the firewall within minutes.

The FVS318v3 VPN Firewall provides the following features:

- Easy, Web-based setup for installation and management.
- Content filtering and site blocking security.
- Built-in eight-port 10/100 Mbps switch.
- Ethernet connection to a WAN device, such as a cable modem or DSL modem.
- Extensive protocol support.
- Login capability.
- Front panel LEDs for easy monitoring of status and activity.
- Flash memory for firmware upgrade.

A Powerful, True Firewall with Content Filtering

Unlike simple Internet sharing NAT firewalls, the FVS318v3 is a true firewall, using stateful packet inspection to defend against hacker attacks. Its firewall features include:

- DoS protection.

  Automatically detects and thwarts DoS attacks such as Ping of Death, SYN Flood, LAND Attack, and IP Spoofing.

- Blocks unwanted traffic from the Internet to your LAN.
- Blocks access from your LAN to Internet locations or services that you specify as off-limits.
- Logs security incidents.

  The FVS318v3 logs security events such as blocked incoming traffic, port scans, attacks, and administrator logins. You can configure the firewall to email the log to you at specified intervals. You can also configure the firewall to send immediate alert messages to your e-mail address or email pager whenever a significant event occurs.

- With its content filtering feature, the FVS318v3 prevents objectionable content from reaching your PCs. The firewall allows you to control access to Internet content by screening for keywords within Web addresses. You can configure the firewall to log and report attempts to access objectionable Internet sites.

Security

The FVS318v3 VPN Firewall is equipped with several features designed to maintain security, as described in this section.

- PCs Hidden by NAT
  NAT opens a temporary path to the Internet for requests originating from the local network. Requests originating from outside the LAN are discarded, preventing users outside the LAN from finding and directly accessing the PCs on the LAN.

- Port Forwarding with NAT
  Although NAT prevents Internet locations from directly accessing the PCs on the LAN, the firewall allows you to direct incoming traffic to specific PCs based on the service port number of the incoming request, or to one designated “DNS” host computer. You can specify forwarding of single ports or ranges of ports.

Autosensing Ethernet Connections with Auto Uplink

With its internal eight-port 10/100 switch, the FVS318v3 can connect to either a 10 Mbps standard Ethernet network or a 100 Mbps Fast Ethernet network. Both the LAN and WAN interfaces are autosensing and capable of full-duplex or half-duplex operation.

The firewall incorporates Auto Uplink™ technology. Each Ethernet port automatically senses whether the Ethernet cable plugged into the port should have a normal connection such as to a PC or an uplink connection such as to a switch or hub. That port then configures itself to the correct configuration. This feature also eliminates the need to worry about crossover cables, as Auto Uplink will accommodate either type of cable to make the right connection.

Extensive Protocol Support

The FVS318v3 VPN Firewall supports the Transmission Control Protocol/Internet Protocol (TCP/IP) and Routing Information Protocol (RIP). For further information about TCP/IP, refer to Appendix B, "Network, Routing, and Firewall Basics."

- IP Address Sharing by NAT
  The FVS318v3 VPN Firewall allows several networked PCs to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your Internet service provider (ISP). This technique, known as NAT, allows the use of an inexpensive single-user ISP account.
- Automatic Configuration of Attached PCs by DHCP
  The FVS318v3 VPN Firewall dynamically assigns network configuration information, including IP, gateway, and Domain Name Server (DNS) addresses, to attached PCs on the LAN using the Dynamic Host Configuration Protocol (DHCP). This feature greatly simplifies configuration of PCs on your local network.
- DNS Proxy
  When DHCP is enabled and no DNS addresses are specified, the firewall provides its own address as a DNS server to the attached PCs. The firewall obtains actual DNS addresses from the ISP during connection setup and forwards DNS requests from the LAN.
- Point-to-Point Protocol over Ethernet (PPPoE)
  PPPoE is a protocol for connecting remote hosts to the Internet over a DSL connection by simulating a dial-up connection. This feature eliminates the need to run a login program such as Entersys or WinPOET on your PC.

Easy Installation and Management

You can install, configure, and operate the FVS318v3 ProSafe VPN Firewall within minutes after connecting it to the network. The following features simplify installation and management tasks:

- Browser-based management
  Browser-based configuration allows you to easily configure your firewall from almost any type of personal computer, such as Windows, Macintosh, or Linux. A user-friendly Setup Wizard is provided and online help documentation is built into the browser-based Web Management Interface.
- Smart Wizard
  The FVS318v3 VPN Firewall automatically senses the type of Internet connection, asking you only for the information required for your type of ISP account.
- Diagnostic functions
  The firewall incorporates built-in diagnostic functions such as Ping, DNS lookup, and remote reboot.
- Remote management
  The firewall allows you to login to the Web Management Interface from a remote location on the Internet. For security, you can limit remote management access to a specified remote IP address or range of addresses, and you can choose a nonstandard port number.
- Visual monitoring
  The FVS318v3 VPN Firewall's front panel LEDs provide an easy way to monitor its status and activity.

Maintenance and Support

NETGEAR offers the following features to help you maximize your use of the FVS318v3 VPN Firewall:

- Flash memory for firmware upgrade.
- Free technical support seven days a week, 24 hours a day.

	Note: The FVS318v3 firmware is not backward compatible with earlier versions of the FVS318 firewall.

Package Contents

The product package should contain the following items:

- FVS318v3 ProSafe VPN Firewall.
- AC power adapter.
- Category 5 (Cat 5) Ethernet cable.
- Installation Guide.
- *Resource CD (240-10114-02) for ProSafe VPN Firewall*, including:
  - This guide.
  - Application Notes and other helpful information.
- Registration and Warranty Card.

If any of the parts are incorrect, missing, or damaged, contact your NETGEAR dealer. Keep the carton, including the original packing materials, in case you need to return the firewall for repair.

The FVS318v3 Front Panel

The front panel of the FVS318v3 VPN Firewall contains the status LEDs described below.

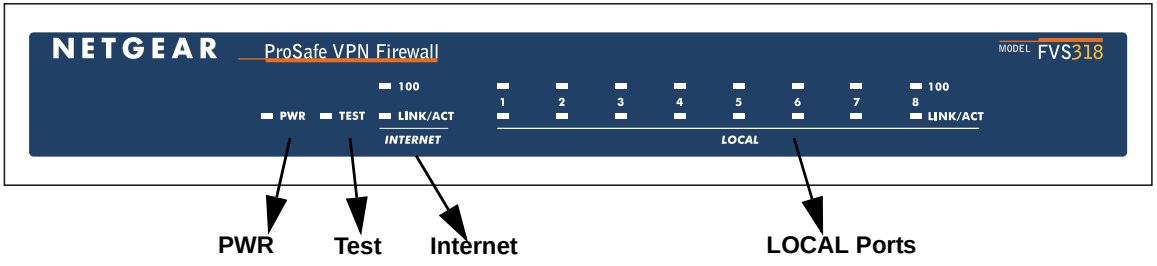


Figure 2-1: FVS318v3 front panel

You can use some of the LEDs to verify connections. Viewed from left to right, Table 2-1 describes the LEDs on the front panel of the firewall. These LEDs are green when lit.

Table 2-1. LED Descriptions

LED Label	Activity	Description
PWR	On	Power is supplied to the firewall.
TEST	On Off	The system is initializing. The system is ready and running.
INTERNET		
100 (100 Mbps)	On Off	The Internet (WAN) port is operating at 100 Mbps. The Internet (WAN) port is operating at 10 Mbps.
LINK/ACT (Link/Activity)	On Blinking	The Internet port has detected a link with an attached device. Data is being transmitted or received by the Internet port.
LOCAL		
100 (100 Mbps)	On Off	The Local port is operating at 100 Mbps. The Local port is operating at 10 Mbps.
LINK/ACT (Link/Activity)	On Blinking	The Local port has detected a link with an attached device. Data is being transmitted or received by the Local port.

The FVS318v3 Rear Panel

The rear panel of the FVS318v3 VPN Firewall contains the port connections listed below.

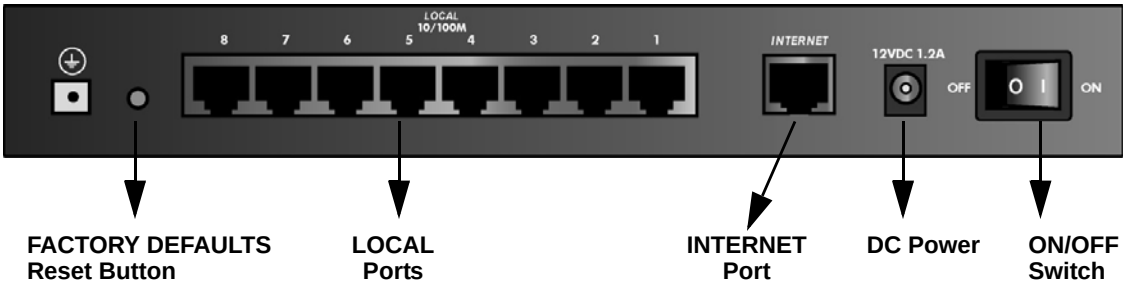


Figure 2-2: FVS318v3 rear panel

Viewed from left to right, the rear panel contains the following features:

- Factory default reset push button
- Eight Ethernet LAN ports
- Internet Ethernet WAN port for connecting the firewall to a cable or DSL modem

- DC power input
- ON/OFF switch

NETGEAR-Related Products

NETGEAR products related to the FVS318v3 are listed in the following table:

Table 2-2. NETGEAR-Related Products

Category	Wireless	Wired
Notebooks	WAG511 108 Mbps Dual Band PC Card WG511T 108 Mbps PC Card WG511 54 Mbps PC Card WG111 54 Mbps USB 2.0 Adapter MA521 802.11b PC Card MA111 802.11b USB Adapter	FA511 CardBus Adapter FA120 USB 2.0 Adapter
Desktops	WAG311 108 Mbps Dual Band PCI Adapter WG311T 108 Mbps PCI Adapter WG311 54 Mbps PCI Adapter WG111 54 Mbps USB 2.0 Adapter MA111 802.11b USB Adapter	FA311 PCI Adapter FA120 USB 2.0 Adapter
PDAs	MA701 802.11b Compact Flash Card	
Antennas and Accessories	ANT24O5 5 dBi Antenna ANT2409 Indoor/Outdoor 9 dBi Antenna ANT24D18 Indoor/Outdoor 18 dBi Antenna Antenna Cables–1.5, 3, 5, 10, and 30 m lengths VPN01L and VPN05L ProSafe VPN Client Software	

NETGEAR Product Registration, Support, and Documentation

Register your product at *http://www.NETGEAR.com/register*. Registration is required before you can use our telephone support service.

Product updates and Web support are always available by going to: *http://kbserver.netgear.com*.

Documentation is available on the *Resource CD* and at *http://kbserver.netgear.com*.

When the VPN firewall router is connected to the Internet, click the **Knowledge Base** or the **Documentation** link under the Web Support menu to view support information or the documentation for the VPN firewall router.

Chapter 3
Connecting the Firewall to the Internet

This chapter describes how to set up the firewall on your LAN, connect to the Internet, perform basic configuration of your FVS318v3 ProSafe VPN Firewall using the Setup Wizard, or how to manually configure your Internet connection.

Follow these instructions to set up your firewall.

Prepare to Install Your FVS318v3 ProSafe VPN Firewall

- *For Cable Modem Service*: When you perform the VPN firewall router setup steps be sure to use the computer you first registered with your cable ISP.
- *For DSL Service*: You may need information such as the DSL login name/e-mail address and password in order to complete the VPN firewall router setup.

Before proceeding with the VPN firewall router installation, familiarize yourself with the contents of the *Resource CD (240-10114-02) for ProSafe VPN Firewall*, especially this manual and the animated tutorials for configuring networking on PCs.

First, Connect the FVS318v3

1. Connect the cables between the FVS318v3, computer, and modem

a. Turn off your computer.

b. Turn off the cable or DSL broadband modem.

c. Locate the Ethernet cable (Cable 1 in the diagram) that connects your PC to the modem.

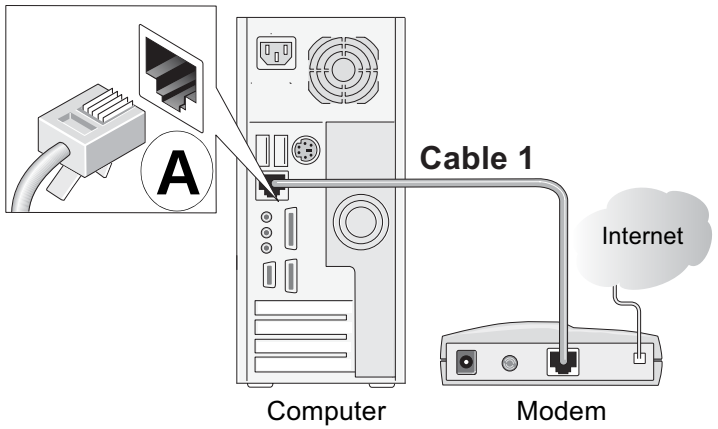


Figure 3-1: Disconnect the Ethernet cable from the computer

d. Disconnect the cable at the computer end only, point **A** in the diagram.

e. Look at the label on the bottom of the VPN firewall router. Locate the Internet port. Securely insert the Ethernet cable from your modem (Cable 1 in the diagram below) into the Internet port of the VPN firewall router as shown in point **B** of the diagram.

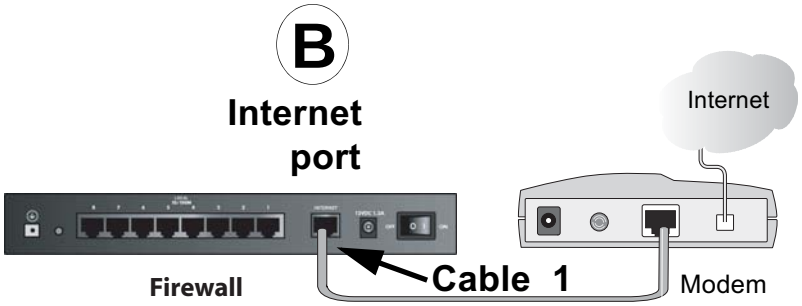


Figure 3-2: Connect the VPN firewall router to the modem

f. Securely insert the blue cable that came with your VPN firewall router (the blue NETGEAR cable in the diagram below) into a LOCAL port on the firewall such as LOCAL port 8 (point **C** in the diagram), and the other end into the Ethernet port of your computer (point **D** in the diagram).

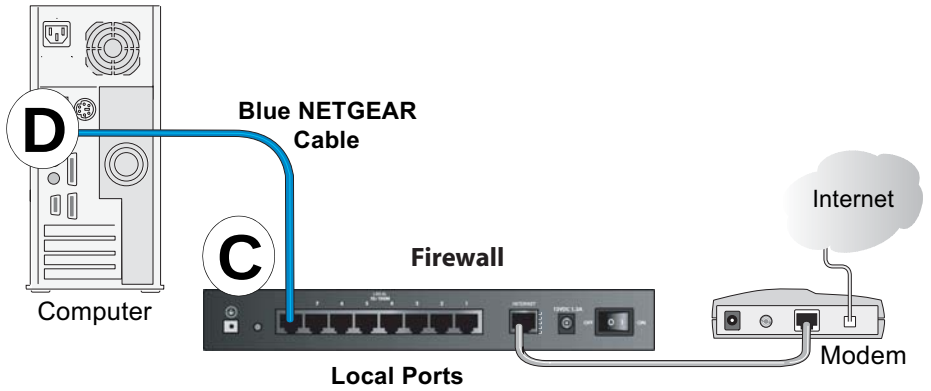


Figure 3-3: Connect the computer to the VPN firewall router

Your network cables are connected and you are ready to restart your network.

2. RESTART YOUR NETWORK IN THE CORRECT SEQUENCE

Warning: Failure to restart your network in the correct sequence could prevent you from connecting to the Internet.

a. First, turn on the broadband modem and wait two minutes.

b. Now, plug in the power cord to your VPN firewall router and wait one minute.

c. Last, turn on your computer.

Note: For DSL customers, if software logs you in to the Internet, *do not* run that software. You may need to go to the Internet Explorer Tools menu, Internet Options, Connections tab page where you can select "Never dial a connection."

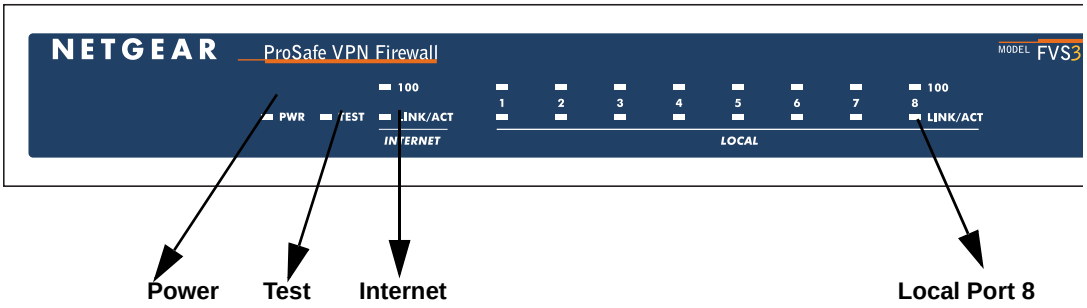


Figure 3-4: Status lights

d. Check the VPN firewall router status lights to verify the following:

- *PWR*: The power light should turn solid green. If it does not, see "Troubleshooting Tips" on page 3-6.
- *TEST:* The test light blinks when the firewall is first turned on then goes off. If after two minutes it is still on, see "Troubleshooting Tips" on page 3-6.
- *INTERNET*: The Internet LINK light should be lit. If not, make sure the Ethernet cable is securely attached to the VPN firewall router Internet port and the modem, and the modem is powered on.
- *LOCAL*: A LOCAL light should be lit. Green on the 100 line indicates your computer is communicating at 100 Mbps; off on the 100 line indicates 10 Mbps. If a LOCAL light is not lit, check that the Ethernet cable from the computer to the firewall is securely attached at both ends, and that the computer is turned on.

Now, Configure the FVS318v3 for Internet Access

1. From the Ethernet connected PC you just set up, open a browser such as Internet Explorer or Netscape® Navigator.

With the VPN firewall router in its factory default state, your browser will automatically display the NETGEAR Smart Wizard Configuration Assistant welcome page.

Figure 3-5: NETGEAR Smart Wizard Configuration Assistant welcome screen

Note: If you do not see this page, type **http://www.routerlogin.net** in the browser address bar and press **Enter**. If you still cannot see this screen, see "How to Bypass the Configuration Assistant" on page 3-10.

If you cannot connect to the VPN firewall router, verify your computer networking setup. It should be set to obtain *both* IP and DNS server addresses automatically, which is usually so. For help with this, see Appendix D, "Preparing Your Network or the animated tutorials on the *Resource CD.*

2. Click **OK**. Follow the prompts to proceed with the Smart Wizard Configuration Assistant to connect to the Internet.

3. Click **Done** to finish. If you have trouble connecting to the Internet, see "Troubleshooting Tips" on page 3-6 to correct basic problems.

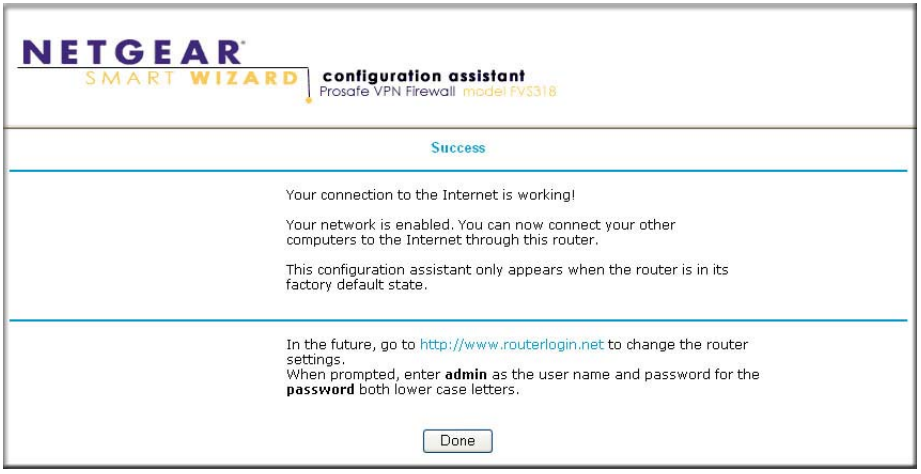

NETGEAR
SMART WIZARD
configuration assistant
Prosafe VPN Firewall model FVS318
Success
Your connection to the Internet is working!
Your network is enabled. You can now connect your other computers to the Internet through this router.
This configuration assistant only appears when the router is in its factory default state.
In the future, go to http://www.routerlogin.net to change the router settings.
When prompted, enter admin as the user name and password for the password both lower case letters.
Done

Figure 3-6: NETGEAR Smart Wizard Configuration Assistant success screen

Note: The Smart Wizard Configuration Assistant only appears when the firewall is in its factory default state. After you configure the VPN firewall router, it will not appear again. You can always connect to the firewall to change its settings. To do so, open a browser such as Internet Explorer and go to **http://www.routerlogin.net**. Then, when prompted, enter **admin** as the user name and **password** for the password both in lower case letters.

You are now connected to the Internet!

Troubleshooting Tips

Here are some tips for correcting simple problems you may have.

Be sure to restart your network in this sequence:

1. Turn off the VPN firewall router, shut down the computer, and unplug and turn off the modem.
2. Turn on the modem and wait two minutes
3. Turn on the VPN firewall router and wait one minute
4. Turn on the computer.

Make sure the Ethernet cables are securely plugged in.

- The Internet link light on the VPN firewall router will be lit if the Ethernet cable to the VPN firewall router from the modem is plugged in securely and the modem and VPN firewall router are turned on.
- For each powered on computer connected to the VPN firewall router with a securely plugged in Ethernet cable, the corresponding VPN firewall router LOCAL port link light will be lit. The labels on the front and back of the VPN firewall router identify the number of each LOCAL port.

Make sure the network settings of the computer are correct.

- LAN connected computers *must* be configured to obtain an IP address automatically via DHCP. Please see Appendix D, "Preparing Your Network or the animated tutorials on the *Resource CD* for help with this.
- Some cable modem ISPs require you to use the MAC address of the computer registered on the account. If so, in the Router MAC Address section of the Basic Settings menu, select "Use this Computer's MAC Address." The firewall will then capture and use the MAC address of the computer that you are now using. You must be using the computer that is registered with the ISP. Click **Apply** to save your settings. Restart the network in the correct sequence.

Use the status lights on the front of the FVS318v3 to verify correct firewall operation.

If the FVS318v3 power light does not turn solid green or if the test light does not go off within two minutes after turning the firewall on, reset the firewall according to the instructions in "Backing Up the Configuration" on page 7-7.

Overview of How to Access the FVS318v3 VPN Firewall

The table below describes how you access the VPN firewall router, depending on the state of the VPN firewall router.

Table 3-1. Ways to access the firewall

Firewall State	Access Options	Description
Factory Default **Note**: The VPN firewall router is supplied in the factory default state. Also, the factory default state is restored when you use the factory reset button. See "Backing Up the Configuration" on page 7-7 for more information on this feature.	Automatic Access via the Smart Wizard Configuration Assistant	Any time a browser is opened on any computer connected to the VPN firewall router, the VPN firewall router will automatically connect to that browser and display the Configuration Assistant welcome page. There is no need to enter the VPN firewall router URL in the browser, or provide the login user name and password.
	Manually enter a URL to bypass the Smart Wizard Configuration Assistant	You can bypass the Smart Wizard Configuration Assistant feature by typing *http://www.routerlogin.net/basicsetting.htm* in the browser address bar and pressing **Enter**. You will not be prompted for a user name or password. This will enable you to manually configure the VPN firewall router even when it is in the factory default state. When manually configuring the firewall, you must complete the configuration by clicking **Apply** when you finish entering your settings. If you do not do so, a browser on any PC connected to the firewall will automatically display the firewall's Configuration Assistant welcome page rather than the browser's home page.
Configuration Settings Have Been Applied	Enter the standard URL to access the VPN firewall router	Connect to the VPN firewall router by typing either of these URLs in the address field of your browser, then press **Enter**: *http://www.routerlogin.net* *http://www.routerlogin.com* The VPN firewall router will prompt you to enter the user name of **admin** and the **password**. The default password is password.
	Enter the IP address of the VPN firewall router	Connect to the VPN firewall router by typing the IP address of the VPN firewall router in the address field of your browser, then press **Enter**. 192.168.0.1 is the default IP address of the VPN firewall router. The VPN firewall router will prompt you to enter the user name of **admin** and the **password**. The default password is password.

How to Log On to the FVS318v3 After Configuration Settings Have Been Applied

1. Connect to the VPN firewall router by typing **http://www.routerlogin.net** in the address field of your browser, then press **Enter**.

Figure 3-7: Login URL

2. For security reasons, the firewall has its own user name and password. When prompted, enter **admin** for the firewall user name and **password** for the firewall password, both in lower case letters. To change the password, see "Changing the Administrator Password" on page 7-8

   Note: The firewall user name and password are not the same as any user name or password you may use to log in to your Internet connection.

   A login window like the one shown below opens:

Figure 3-8: Login window

   Once you have entered your user name and password, your Web browser should find the FVS318v3 VPN Firewall and display the home page as shown below.

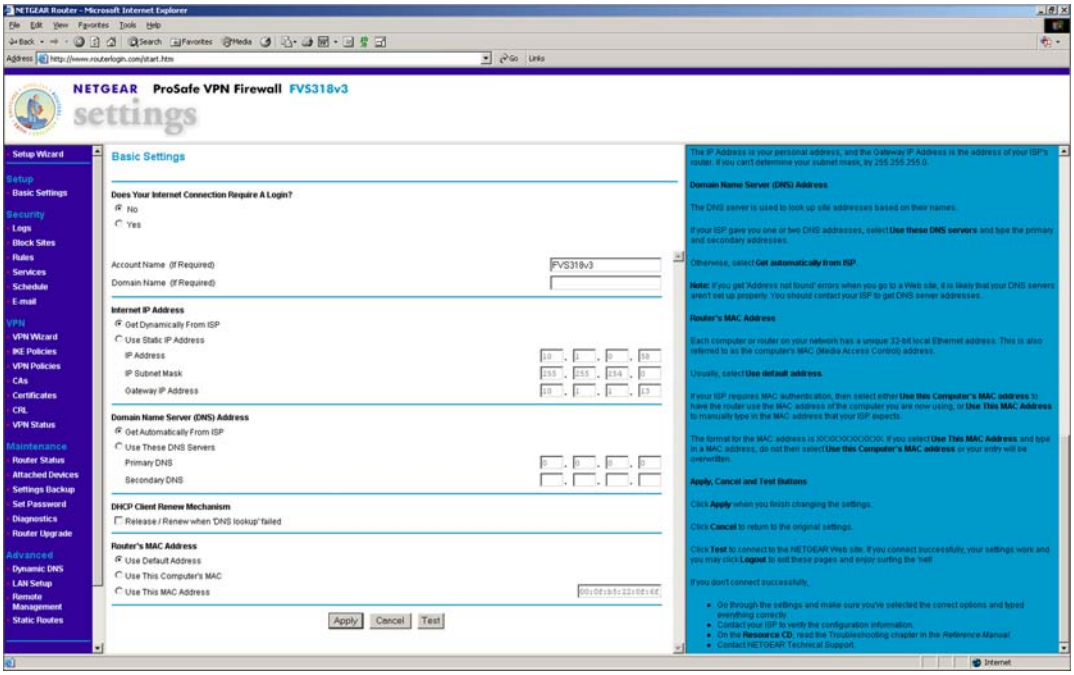


Figure 3-9: Login result: FVS318v3 home page

When the VPN firewall router is connected to the Internet, click the **Knowledge Base** or the **Documentation** link under the Web Support menu to view support information or the documentation for the VPN firewall router.

If you do not click **Logout**, the VPN firewall router will wait five minutes after there is no activity before it automatically logs you out.

How to Bypass the Configuration Assistant

1. When the VPN firewall router is in the factory default state, type **http://www.routerlogin.net/basicsetting.htm** in your browser, then press **Enter**.

   When the VPN firewall router is in the factory default state, a user name and password are not required.

2. The browser then displays the FVS318v3 settings home page shown in “Login result: FVS318v3 home page” on page 3-10.

If you do not click **Logout**, the VPN firewall router waits five minutes after there is no activity before it automatically logs you out.

Using the Smart Setup Wizard

You can use the Smart Setup Wizard to assist with manual configuration or to verify the Internet connection. The Smart Setup Wizard is not the same as the Smart Wizard Configuration Assistant (as illustrated in Figure 3-5) that only appears when the firewall is in its factory default state. After you configure the VPN firewall router, the Smart Wizard Configuration Assistant will not appear again.

To use the Smart Setup Wizard to assist with manual configuration or to verify the Internet connection settings, follow this procedure.

1. Connect to the VPN firewall router by typing **http://www.routerlogin.net** in the address field of your browser, then press **Enter**.
2. For security reasons, the firewall has its own user name and password. When prompted, enter **admin** for the firewall user name and **password** for the firewall password, both in lower case letters. To change the password, see "Changing the Administrator Password" on page 7-8

   Note: The firewall user name and password are not the same as any user name or password you may use to log in to your Internet connection.

   Once you have entered your user name and password, your Web browser should find the FVS318v3 VPN Firewall and display the home page as shown in Figure 3-9.
3. Click **Setup Wizard** on the upper left of the main menu.
4. Click **Next** to proceed. Input your ISP settings, as needed.
5. At the end of the Setup Wizard, click the **Test** button to verify your Internet connection. If you have trouble connecting to the Internet, use the Troubleshooting Tips "Troubleshooting Tips" on page 3-6 to correct basic problems, or refer to Chapter 9, "Troubleshooting."

How to Manually Configure Your Internet Connection

You can manually configure your firewall using the menu below, or you can allow the Setup Wizard to determine your configuration as described in the previous section.

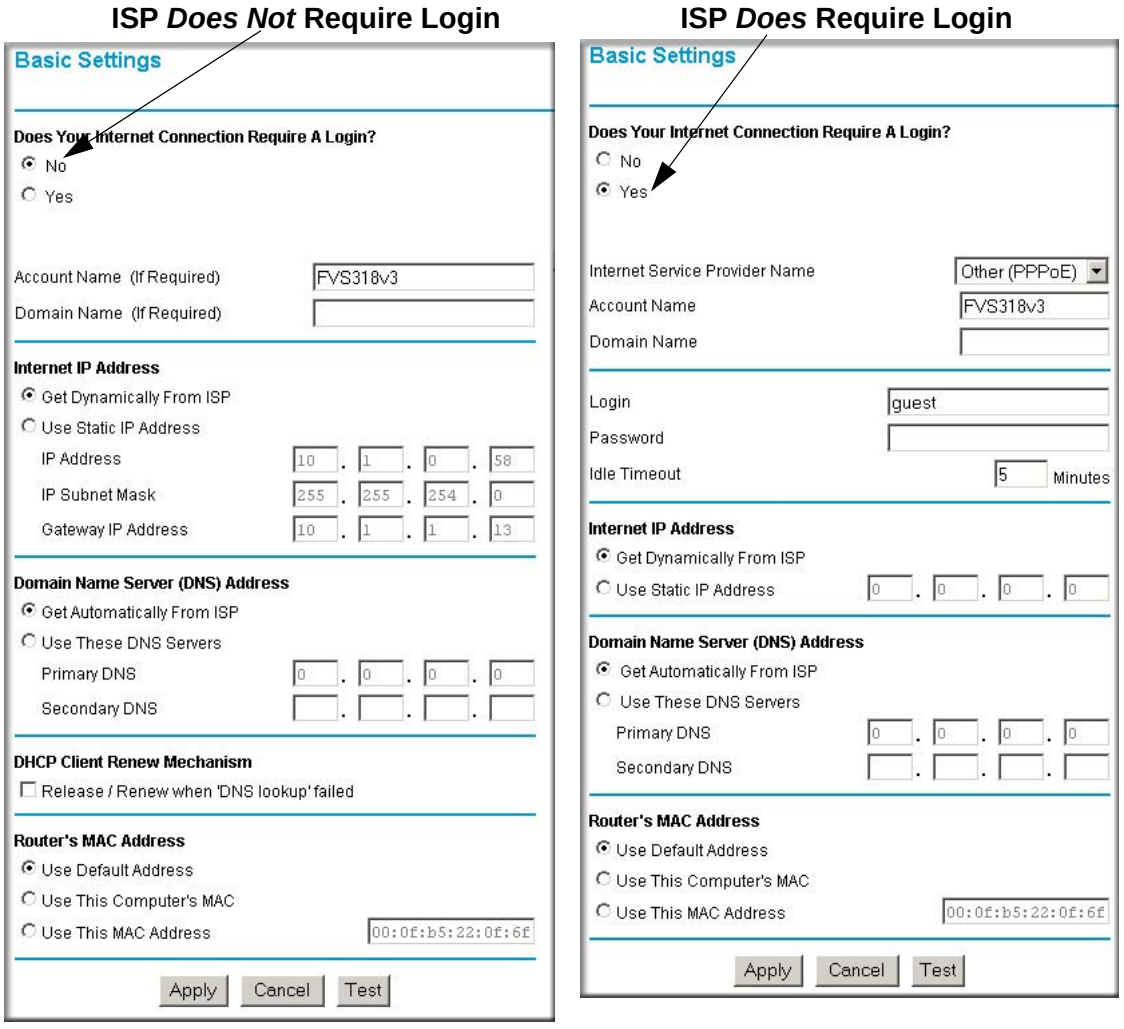


Figure 3-10: Browser-based configuration Basic Settings menu

You can manually configure the firewall using the Basic Settings menu shown in Figure 3-10 using these steps:

1. Log in to the firewall at its default address of **http://www.routerlogin.net** using a browser like Internet Explorer or Netscape® Navigator.
2. Click the **Basic Settings** link under the **Setup** section of the main menu.
3. If your Internet connection does not require a login, click **No** at the top of the **Basic Settings** menu and fill in the settings according to the instructions below. If your Internet connection does require a login, click **Yes**, and skip to step 4.

   a. Account:
   Enter your Account Name (may also be called Host Name) and Domain Name. These parameters may be necessary to access your ISP's services such as mail or news servers.

   b. Internet IP Address:
   If your ISP has assigned you a permanent, fixed (static) IP address for your PC, select "Use static IP address". Enter the IP address that your ISP assigned. Also enter the netmask and the Gateway IP address. The Gateway is the ISP's firewall to which your firewall will connect.

   c. Domain Name Server (DNS) Address:
   If you know that your ISP does not automatically transmit DNS addresses to the firewall during login, select "Use these DNS servers" and enter the IP address of your ISP's Primary DNS Server. If a Secondary DNS Server address is available, enter it also.

   Note: After completing the DNS configuration, restart the computers on your network so that these settings take effect.

   d. Firewall's MAC Address:
   This section determines the Ethernet MAC address that will be used by the firewall on the Internet port. Some ISPs will register the Ethernet MAC address of the network interface card in your PC when your account is first opened. They will then only accept traffic from the MAC address of that PC. This feature allows your firewall to masquerade as that PC by "cloning" its MAC address.

   To change the MAC address, select "Use this Computer's MAC address." The firewall will then capture and use the MAC address of the PC that you are now using. You must be using the one PC that is allowed by the ISP. Or, select "Use this MAC address" and enter it.

   e. Click **Apply** to save your settings.

4. If your Internet connection does require a login, fill in the settings according to the instructions below. Select Yes if you normally must launch a login program such as Enternet or WinPOET in order to access the Internet.

   Note: After you finish setting up your firewall, you will no longer need to launch the ISP's login program on your PC in order to access the Internet. When you start an Internet application, your firewall will automatically log you in.

   a. For connections that require a login using protocols such as PPPoE, PPTP, Telstra Bigpond Cable broadband connections, select your Internet service provider from the drop-down list.

Figure 3-11: Basic Settings ISP list

   b. The screen will change according to the ISP settings requirements of the ISP you select.

   c. Fill in the parameters for your ISP according to the Wizard-detected procedures starting on page 3-11.

   d. Click **Apply** to save your settings.

Chapter 4
Firewall Protection and Content Filtering

This chapter describes how to use the content filtering features of the FVS318v3 ProSafe VPN Firewall to protect your network. These features can be found by clicking on the **Security** heading in the main menu of the browser interface.

Firewall Protection and Content Filtering Overview

The FVS318v3 ProSafe VPN Firewall provides you with Web content filtering options, plus browsing activity reporting and instant alerts via e-mail. Parents and network administrators can establish restricted access policies based on time-of-day, Web addresses and Web address keywords. You can also block Internet access by applications and services, such as chat or games.

A firewall is a special category of router that protects one network (the trusted network, such as your LAN) from another (the untrusted network, such as the Internet), while allowing communication between the two. A firewall incorporates the functions of a NAT (Network Address Translation) router, while adding features for dealing with a hacker intrusion or attack, and for controlling the types of traffic that can flow between the two networks. Unlike simple Internet sharing NAT routers, a firewall uses a process called stateful packet inspection to protect your network from attacks and intrusions. NAT performs a very limited stateful inspection in that it considers whether the incoming packet is in response to an outgoing request, but true stateful packet inspection goes far beyond NAT.

To configure these features of your firewall, click on the subheadings under the **Security** heading in the main menu of the browser interface. The subheadings are described below:

Block Sites

The FVS318v3 allows you to restrict access based on Web addresses and Web address keywords. Up to 255 entries are supported in the Keyword list. The Block Sites menu is shown in Figure 4-1:

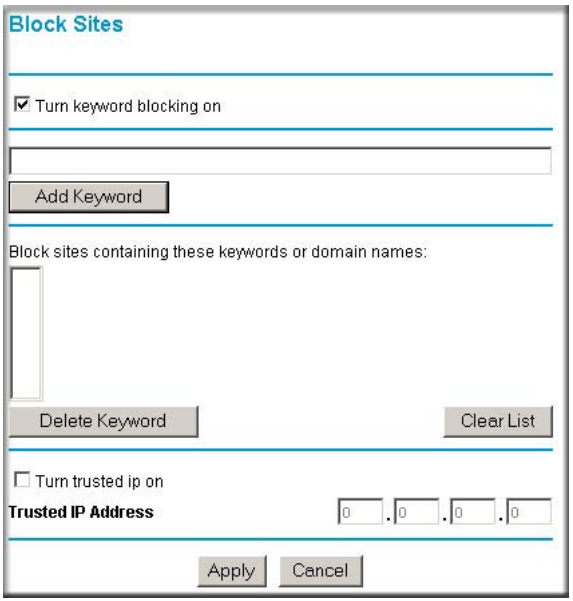


Figure 4-1: Block Sites menu

To enable keyword blocking, check **Turn keyword blocking on**, then click **Apply**.

To add a keyword or domain, type it in the Keyword box, click **Add Keyword**, then click **Apply**.

To delete a keyword or domain, select it from the list, click **Delete Keyword**, then click **Apply**.

Keyword application examples:

- If the keyword "XXX" is specified, the URL <http://www.badstuff.com/xxx.html> is blocked, as is the newsgroup alt.pictures.XXX.
- If the keyword ".com" is specified, only Web sites with other domain suffixes (such as .edu or .gov) can be viewed.
- If you wish to block all Internet browsing access, enter the keyword ".".

To specify a Trusted User, enter that PC's IP address in the **Trusted User** box and click **Apply**.

You may specify one Trusted User, which is a PC that will be exempt from blocking and logging. Since the Trusted User will be identified by an IP address, you should configure that PC with a fixed or reserved IP address.

Using Rules to Block or Allow Specific Kinds of Traffic

Firewall rules are used to block or allow specific traffic passing through from one side to the other. Inbound rules (WAN to LAN) restrict access by outsiders to private resources, selectively allowing only specific outside users to access specific resources. Outbound rules (LAN to WAN) determine what outside resources local users can have access to.

A firewall has two default rules, one for inbound traffic and one for outbound. The default rules of the FVS318v3 are:

- Inbound: Block all access from outside except responses to requests from the LAN side.
- Outbound: Allow all access from the LAN side to the outside.

These default rules are shown in the Rules table of the Rules menu in Figure 4-2:

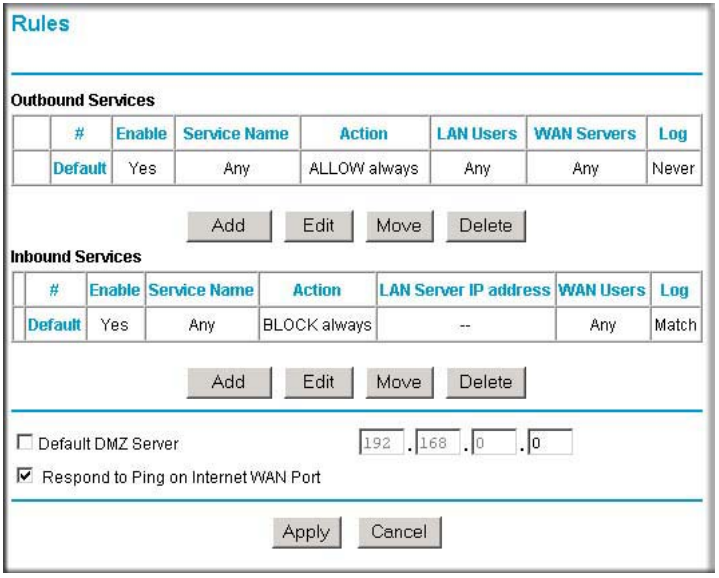

Rules
Outbound Services
Enable Service Name Action LAN Users WAN Servers Log
Default Yes Any ALLOW always Any Any Never
Add Edit Move Delete
Inbound Services
Enable Service Name Action LAN Server IP address WAN Users Log
Default Yes Any BLOCK always -- Any Match
Add Edit Move Delete
Default DMZ Server
192 . 168 . 0 . 0
Respond to Ping on Internet WAN Port
Apply Cancel

Figure 4-2: Rules menu

You may define additional rules that specify exceptions to the default rules. By adding custom rules, you can block or allow access based on the service or application, source or destination IP addresses, and time of day. You can also choose to log traffic that matches or does not match the rule you have defined.

To create a new rule, click the **Add** button.

To edit an existing rule, select its button on the left side of the table and click **Edit**.

To delete an existing rule, select its button on the left side of the table and click **Delete**.

To move an existing rule to a different position in the table, select its button on the left side of the table and click **Move**. At the script prompt, enter the number of the desired new position and click **OK**.

An example of the menu for defining or editing a rule is shown in Figure 4-3. The parameters are:

- **Service**. From this list, select the application or service to be allowed or blocked. The list already displays many common services, but you are not limited to these choices. Use the Services menu to add any additional services or applications that do not already appear.
- **Action**. Choose how you would like this type of traffic to be handled. You can block or allow always, or you can choose to block or allow according to the schedule you have defined in the Schedule menu.
- **Source Address**. Specify traffic originating on the LAN (outbound) or the WAN (inbound), and choose whether you would like the traffic to be restricted by source IP address. You can select Any, a Single address, or a Range. If you select a range of addresses, enter the range in the start and finish boxes. If you select a single address, enter it in the start box.
- **Destination Address**.The Destination Address will be assumed to be from the opposite (LAN or WAN) of the Source Address. As with the Source Address, you can select Any, a Single address, or a Range unless NAT is enabled and the destination is the LAN. In that case, you must enter a Single LAN address in the start box.
- **Log**. You can select whether the traffic will be logged. The choices are:
  - Never — no log entries will be made for this service.
  - Match — traffic of this type that matches the parameters and action will be logged.

Inbound Rules (Port Forwarding)

Because the FVS318v3 uses Network Address Translation (NAT), your network presents only one IP address to the Internet, and outside users cannot directly address any of your local computers. However, by defining an inbound rule you can make a local server (for example, a Web server or game server) visible and available to the Internet. The rule tells the firewall to direct inbound traffic for a particular service to one local server based on the destination port number. This is also known as port forwarding.

Note: Some residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to the Acceptable Use Policy of your ISP.

Remember that allowing inbound services opens holes in your FVS318v3 VPN Firewall. Only enable those ports that are necessary for your network. Following are two application examples of inbound rules:

Inbound Rule Example: A Local Public Web Server

If you host a public Web server on your local network, you can define a rule to allow inbound Web (HTTP) requests from any outside IP address to the IP address of your Web server at any time of day. This rule is shown in Figure 4-3:

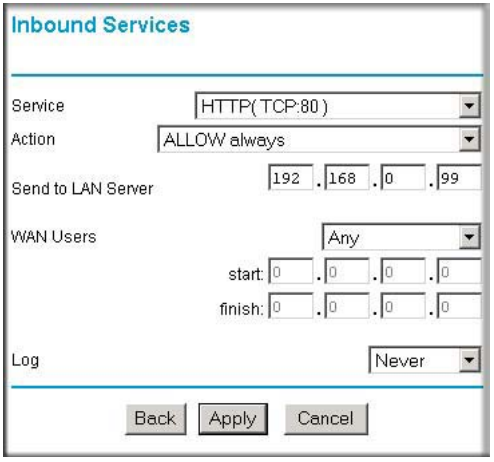


Figure 4-3: Rule example: a local public Web server

Inbound Rule Example: Allowing a Videoconference from Restricted Addresses

If you want to allow incoming videoconferencing to be initiated from a restricted range of outside IP addresses, such as from a branch office, you can create an inbound rule. In the example shown in Figure 4-4, CU-SEEME connections are allowed only from a specified range of external IP addresses. In this case, we have also specified logging of any incoming CU-SeeMe requests that do not match the allowed parameters.

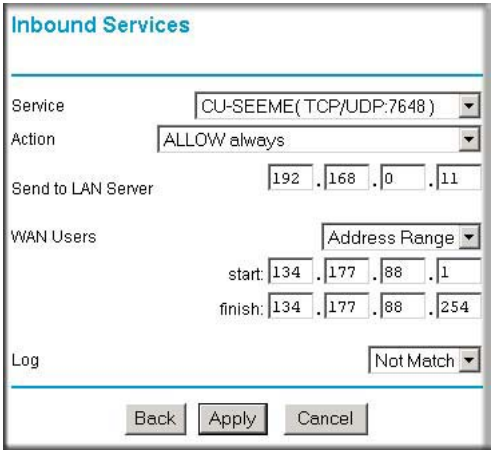


Figure 4-4: Rule example: a videoconference from restricted addresses

Considerations for Inbound Rules

- If your external IP address is assigned dynamically by your ISP, the IP address may change periodically as the DHCP lease expires. Consider using the Dyamic DNS feature in the Advanced menus so that external users can always find your network.
- If the IP address of the local server PC is assigned by DHCP, it may change when the PC is rebooted. To avoid this, use the Reserved IP address feature in the LAN IP menu to keep the PC's IP address constant.
- Each local PC must access the local server using the PC's local LAN address (192.168.0.99 in this example). Attempts by local PCs to access the server using the external WAN IP address will fail.

Outbound Rules (Service Blocking)

The FVS318v3 allows you to block the use of certain Internet services by PCs on your network. This is called service blocking or port filtering. You can define an outbound rule to block Internet access from a local PC based on:

- IP address of the local PC (source address)
- IP address of the Internet site being contacted (destination address)
- Time of day
- Type of service being requested (service port number)

Following is an application example of an outbound rule:

Outbound Rule Example: Blocking Instant Messenger

If you want to block Instant Messenger usage by employees during working hours, you can create an outbound rule to block that application from any internal IP address to any external address according to the schedule that you have created in the Schedule menu. You can also have the firewall log any attempt to use Instant Messenger during that blocked period.

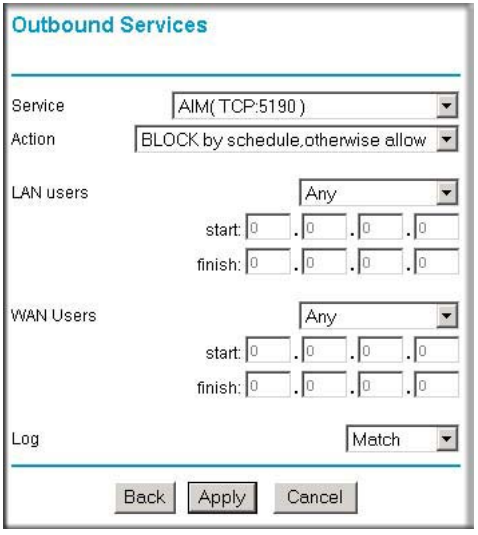


Figure 4-5: Rule example: blocking Instant Messenger

Order of Precedence for Rules

As you define new rules, they are added to the tables in the Rules table, as shown below:

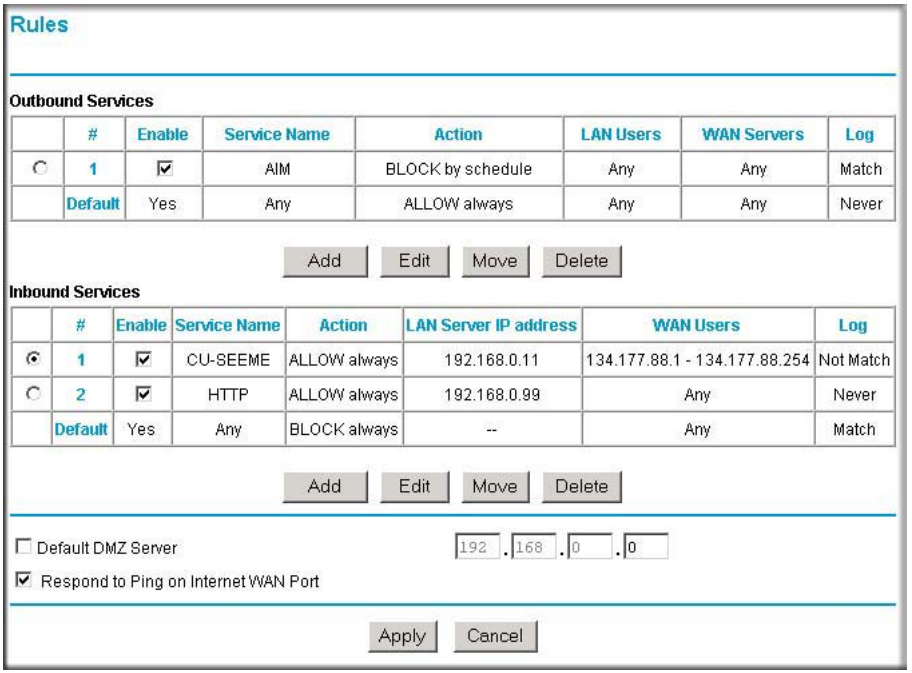

Rules
Outbound Services
Enable Service Name Action LAN Users WAN Servers Log
1 AIM BLOCK by schedule Any Any Match
Default Yes Any ALLOW always Any Any Never
Add Edit Move Delete
Inbound Services
Enable Service Name Action LAN Server IP address WAN Users Log
1 CU-SEEME ALLOW always 192.168.0.11 134.177.88.1 - 134.177.88.254 Not Match
2 HTTP ALLOW always 192.168.0.99 Any Never
Default Yes Any BLOCK always -- Any Match
Add Edit Move Delete
Default DMZ Server
192 . 168 . 0 . 0
Respond to Ping on Internet WAN Port
Apply Cancel

Figure 4-6: Rules table with examples

For any traffic attempting to pass through the firewall, the packet information is subjected to the rules in the order shown in the Rules table, beginning at the top and proceeding to the default rules at the bottom. In some cases, the order of precedence of two or more rules may be important in determining the disposition of a packet. The Move button allows you to relocate a defined rule to a new position in the table.

Default DMZ Server

Incoming traffic from the Internet is normally discarded by the firewall unless the traffic is a response to one of your local computers or a service for which you have configured an inbound rule. Instead of discarding this traffic, you can have it forwarded to one computer on your network. This computer is called the Default DMZ Server.

The Default DMZ Server feature is helpful when using some online games and videoconferencing applications that are incompatible with NAT. The firewall is programmed to recognize some of these applications and to work properly with them, but there are other applications that may not function well. In some cases, one local PC can run the application properly if that PC's IP address is entered as the Default DMZ Server.

Note: For security, NETGEAR strongly recommends that you avoid using the Default DMZ Server feature. When a computer is designated as the Default DMZ Server, it loses much of the protection of the firewall, and is exposed to many exploits from the Internet. If compromised, the computer can be used to attack your network.

To assign a computer or server to be a Default DMZ server:

1. Click **Default DMZ Server**.
2. Type the IP address for that server.
3. Click **Apply**.

Note: In this application, the use of the term "DMZ" has become common, although it is a misnomer. In traditional firewalls, a DMZ is actually a separate physical network port. A true DMZ port is for connecting servers that require greater access from the outside, and will therefore be provided with a different level of security by the firewall. A better term for our application is Exposed Host.

Respond to Ping on Internet WAN Port

If you want the firewall to respond to a ping from the Internet, click the **Respond to Ping on Internet WAN Port** check box. This should only be used as a diagnostic tool, since it allows your firewall to be discovered. Don't check this box unless you have a specific reason to do so.

Services

Services are functions performed by server computers at the request of client computers. For example, Web servers serve Web pages, time servers serve time and date information, and game hosts serve data about other players' moves. When a computer on the Internet sends a request for service to a server computer, the requested service is identified by a service or port number. This number appears as the destination port number in the transmitted IP packets. For example, a packet that is sent with destination port number 80 is an HTTP (Web server) request.

The service numbers for many common protocols are defined by the Internet Engineering Task Force (IETF) and published in RFC1700, "Assigned Numbers." Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application.

Although the FVS318v3 already holds a list of many service port numbers, you are not limited to these choices. Use the Services menu to add additional services and applications to the list for use in defining firewall rules. The Services menu shows a list of services that you have defined, as shown in Figure 4-7:

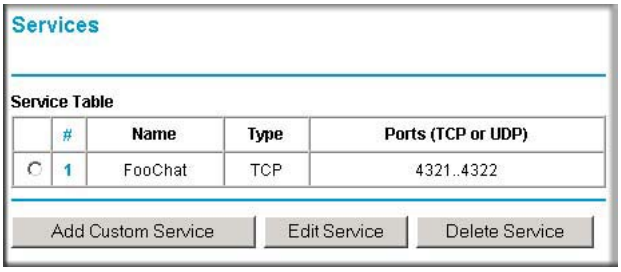


Figure 4-7: Services menu

To define a new service, first you must determine which port number or range of numbers is used by the application. This information can usually be determined by contacting the publisher of the application or from user groups of newsgroups.

To add a service:

1. When you have the port number information, go the Services menu and click on the **Add Custom Service** button. The **Add Services** menu appears as shown in Figure 4-8:

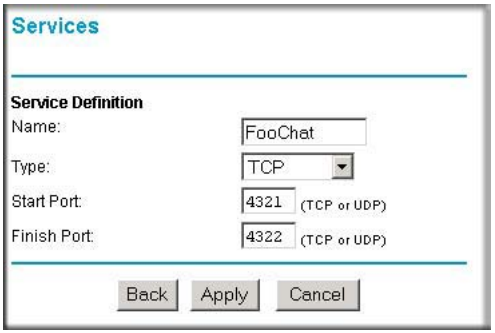


Figure 4-8: Add Custom Service menu

2. Enter a descriptive name for the service so that you will remember what it is.
3. Select whether the service uses TCP or UDP as its transport protocol.
   If you can't determine which is used, select both.
4. Enter the lowest port number used by the service.
5. Enter the highest port number used by the service.
   If the service only uses a single port number, enter the same number in both fields.
6. Click **Apply**.

The new service now appears in the Services menu, and in the Service name selection box in the Rules menu.

Using a Schedule to Block or Allow Specific Traffic

If you enabled content filtering in the Block Sites menu, or if you defined an outbound rule to use a schedule, you can set up a schedule for when blocking occurs or when access is restricted. The firewall allows you to specify when blocking will be enforced by configuring the Schedule page shown below:

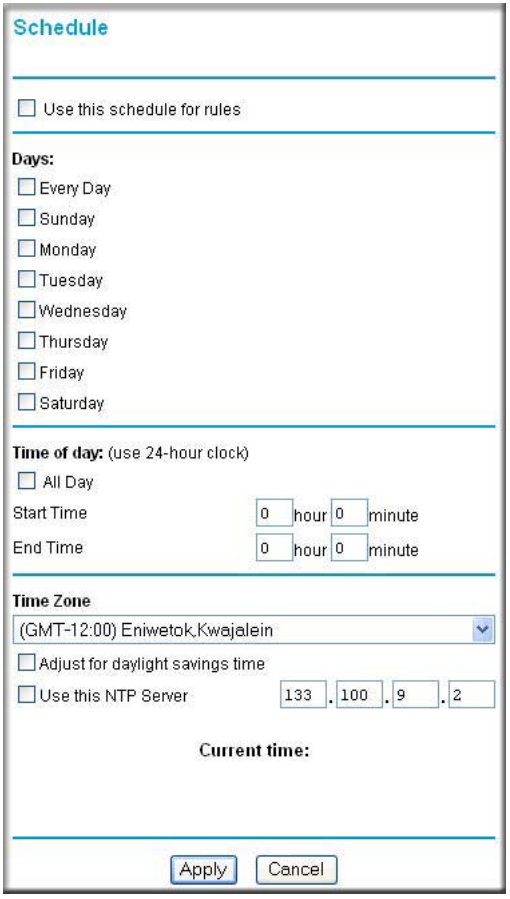


Figure 4-9: Schedule page

To block keywords or Internet domains based on a schedule, select Every Day or select one or more days. If you want to limit access completely for the selected days, select All Day. Otherwise, If you want to limit access during certain times for the selected days, type a Start Blocking time and an End Blocking time.

Note: Enter the values as 24-hour time. For example, to specify 10:30 am, enter 10 hours and 30 minutes; for 10:30 pm, enter 22 hours and 30 minutes.

Be sure to click **Apply** when you have finished configuring this page.

Time Zone

The FVS318v3 VPN Firewall uses the Network Time Protocol (NTP) to obtain the current time and date from one of several Network Time Servers on the Internet. In order to localize the time for your log entries, you must specify your Time Zone:

- Time Zone. Select your local time zone. This setting will be used for the blocking schedule and for time-stamping log entries.
- Daylight Savings Time. Check this box for daylight savings time.

  Note: If your region uses Daylight Savings Time, you must manually select Adjust for Daylight Savings Time on the first day of Daylight Savings Time, and unselect it at the end. Enabling Daylight Savings Time will add one hour to the standard time.

Be sure to click **Apply** when you have finished configuring this menu.

Getting E-Mail Notifications of Event Logs and Alerts

In order to receive logs and alerts by e-mail, you must provide your e-mail information in the Send alerts and logs by e-mail area:

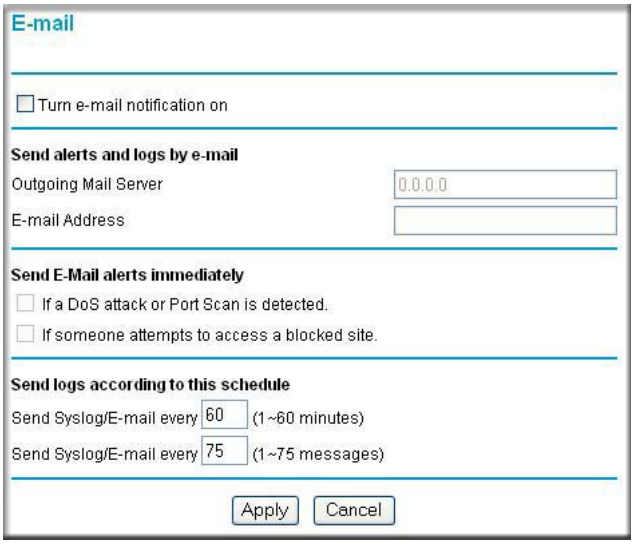

E-mail
Turn e-mail notification on
Send alerts and logs by e-mail
Outgoing Mail Server
0.0.0.0
E-mail Address
Send E-Mail alerts immediately
If a DoS attack or Port Scan is detected.
If someone attempts to access a blocked site.
Send logs according to this schedule
Send Syslog/E-mail every 60 (1~60 minutes)
Send Syslog/E-mail every 75 (1~75 messages)
Apply
Cancel

Figure 4-10: E-mail menu

- **Turn e-mail notification on.** Check this box if you wish to receive e-mail logs and alerts from the firewall.
- **Send alerts and logs by e-mail.** If your enable e-mail notification, these boxes cannot be blank. Enter the name or IP address of your ISP's outgoing (SMTP) mail server (such as mail.myISP.com). You may be able to find this information in the configuration menu of your e-mail program. Enter the e-mail address to which logs and alerts are sent. This e-mail address will also be used as the From address. If you leave this box blank, log and alert messages will not be sent via e-mail.
- **Send E-mail alerts immediately.** You can specify that logs are immediately sent to the specified e-mail address when any of the following events occur:
  - If a Denial of Service attack is detected.
  - If a Port Scan is detected.

  - If a user on your LAN attempts to access a Web site that you blocked using the Block Sites menu.

- **Send logs according to this schedule.** You can specify that logs are sent to you according to a schedule. Select whether you would like to receive the logs None, Hourly, Daily, Weekly, or When Full. Depending on your selection, you may also need to specify:

  - Day for sending log
    Relevant when the log is sent weekly or daily.

  - Time for sending log
    Relevant when the log is sent daily or weekly.

  If the Weekly, Daily or Hourly option is selected and the log fills up before the specified period, the log is automatically e-mailed to the specified e-mail address. After the log is sent, the log is cleared from the firewall's memory. If the firewall cannot e-mail the log file, the log buffer may fill up. In this case, the firewall overwrites the log and discards its contents.

Be sure to click **Apply** when you have finished configuring this menu.

Viewing Logs of Web Access or Attempted Web Access

The firewall logs security-related events such as denied incoming and outgoing service requests, hacker probes, and administrator logins. If you enable content filtering in the Block Sites menu, the Log page will also show you when someone on your network tried to access a blocked site. If you enabled e-mail notification, you'll receive these logs in an e-mail message. If you don't have e-mail notification enabled, you can view the logs here. An example is shown in Figure 4-11:

Logs
Date: 2000-01-01 00:25:34
Destination: 217.207.63.122 - [Unable to determine route to destination, dropping packet Src 1075 Dst 161 from CORP n/w]
Sat, 2000-01-01 00:24:50 - UDP packet - Source: 192.168.0.2 -
Destination: 217.207.63.122 - [Unable to determine route to destination, dropping packet Src 1075 Dst 161 from CORP n/w]
Sat, 2000-01-01 00:25:01 - [Send out NTP Request to 133.100.9.2]
Sat, 2000-01-01 00:25:01 - [NTP Reply Invalid]
Sat, 2000-01-01 00:25:27 - UDP packet - Source: 192.168.0.2 -
Destination: 217.207.63.122 - [Unable to determine route to destination, dropping packet Src 1075 Dst 161 from CORP n/w]
Sat, 2000-01-01 00:25:31 - [Send out NTP Request to 133.100.9.2]
Sat, 2000-01-01 00:25:31 - [NTP Reply Invalid]
Sat, 2000-01-01 00:25:33 - UDP packet - Source: 192.168.0.2 -
Destination: 217.207.63.122 - [Unable to determine route to destination, dropping packet Src 1075 Dst 161 from CORP n/w]
Refresh
Clear Log
Send Log
Include in Log
Known DoS attacks and port scans
Attempted access to blocked sites
Router administration (startup, time sync, logins, etc)
All websites and newsgroups visited
Local activity
All incoming and outgoing traffic
Enable Syslog
Broadcast on LAN
Send to this Syslog Server IP Address
0 . 0 . 0 . 0
Apply
Cancel

Figure 4-11: Logs menu

Log entries are described in Table 4-1

Table 4-1. Log entry descriptions

Field	Description
Date and Time	The date and time the log entry was recorded.
Description or Action	The type of event and what action was taken if any.
Source IP	The IP address of the initiating device for this log entry.
Source port and interface	The service port number of the initiating device, and whether it originated from the LAN or WAN.
Destination	The name or IP address of the destination device or Web site.
Destination port and interface	The service port number of the destination device, and whether it's on the LAN or WAN.

Log action buttons are described in Table 4-2

Table 4-2. Log action buttons

Button	Description
Refresh	Refresh the log screen.
Clear Log	Clear the log entries.
Send Log	Email the log immediately.

Syslog

You can configure the firewall to send system logs to an external PC that is running a syslog logging program. Enter the IP address of the logging PC and click the **Enable Syslog** check box.

Logging programs are available for Windows, Macintosh, and Linux computers.

Chapter 5
Basic Virtual Private Networking

This chapter describes how to use the virtual private networking (VPN) features of the FVS318v3 VPN Firewall. VPN communications paths are called tunnels. VPN tunnels provide secure, encrypted communications between your local network and a remote network or computer.

The VPN information is organized as follows:

- "Overview of VPN Configuration" on page 5-2 provides an overview of the two most common VPN configurations: client-to-gateway and gateway-to-gateway.
- "Planning a VPN" on page 5-3 provides the VPN Committee (VPNC) recommended default parameters set by the VPN Wizard.
- "VPN Tunnel Configuration" on page 5-5 summarizes the two ways to configure a VPN tunnel: VPN Wizard (recommended for most situations) and Advanced (see Chapter 6, "Advanced Virtual Private Networking).
- "How to Set Up a Client-to-Gateway VPN Configuration" on page 5-5 provides the steps needed to configure a VPN tunnel between a remote PC and a network gateway using the VPN Wizard and the NETGEAR ProSafe VPN Client.
- "How to Set Up a Gateway-to-Gateway VPN Configuration" on page 5-20 provides the steps needed to configure a VPN tunnel between two network gateways using the VPN Wizard.
- "VPN Tunnel Control" on page 5-26 provides the step-by-step procedures for activating, verifying, deactivating, and deleting a VPN tunnel once the VPN tunnel has been configured.
- Chapter 6, "Advanced Virtual Private Networking" provides the steps needed to configure VPN tunnels when there are special circumstances and the VPNC recommended defaults of the VPN Wizard are inappropriate.
- Appendix C, "Virtual Private Networking" discusses Virtual Private Networking (VPN) Internet Protocol security (IPSec). IPSec is one of the most complete, secure, and commercially available, standards-based protocols developed for transporting data.
- Appendix E, "VPN Configuration of NETGEAR FVS318v3" presents a case study on how to configure a secure IPSec VPN tunnel from a NETGEAR FVS318v3 to a FVL328. This case study follows the VPN Consortium interoperability profile guidelines (found at *http://www.vpnc.org/InteropProfiles/Interop-01.html*).

Overview of VPN Configuration

Two common scenarios for configuring VPN tunnels are between a remote personal computer and a network gateway and between two or more network gateways. The FVS318v3 supports both of these types of VPN configurations. The FVS318v3 VPN Firewall supports up to eight concurrent tunnels.

Client-to-Gateway VPN Tunnels

Client-to-gateway VPN tunnels provide secure access from a remote PC, such as a telecommuter connecting to an office network (see Figure 5-1).

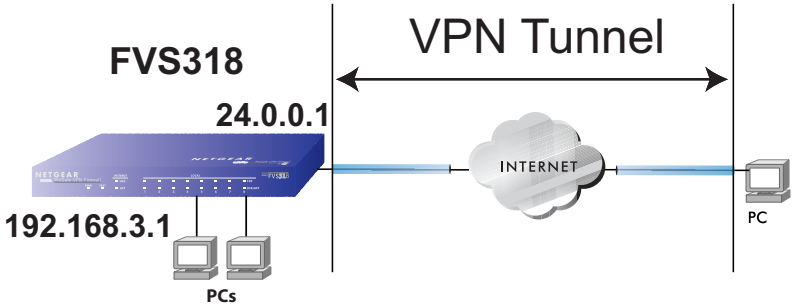


Figure 5-1: Client-to-gateway VPN tunnel

A VPN client access allows a remote PC to connect to your network from any location on the Internet. In this case, the remote PC is one tunnel endpoint, running the VPN client software. The FVS318v3 VPN Firewall on your network is the other tunnel endpoint. See "How to Set Up a Client-to-Gateway VPN Configuration" on page 5-5 to set up this configuration.

Gateway-to-Gateway VPN Tunnels

- Gateway-to-gateway VPN tunnels provide secure access between networks, such as a branch or home office and a main office (see Figure 5-2).

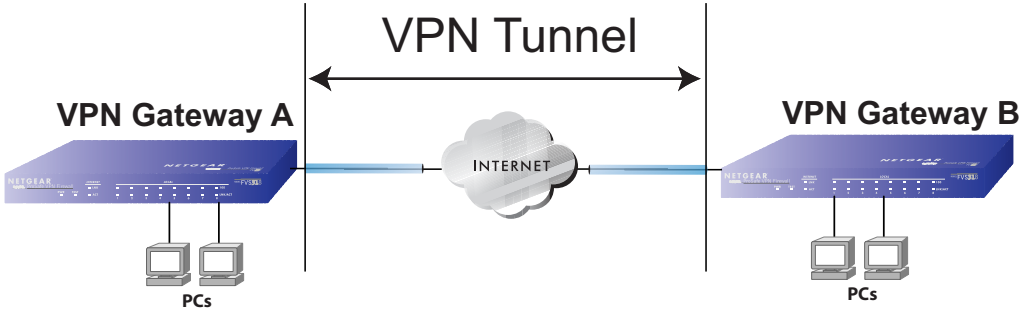


Figure 5-2: Gateway-to-gateway VPN tunnel

A VPN between two or more NETGEAR VPN-enabled firewalls is a good way to connect branch or home offices and business partners over the Internet. VPN tunnels also enable access to network resources across the Internet. In this case, use FVS318v3s on each end of the tunnel to form the VPN tunnel end points. See "How to Set Up a Gateway-to-Gateway VPN Configuration" on page 5-20 to set up this configuration.

Planning a VPN

To set up a VPN connection, you must configure each endpoint with specific identification and connection information describing the other endpoint. You must configure the outbound VPN settings on one end to match the inbound VPN settings on other end, and vice versa.

This set of configuration information defines a security association (SA) between the two VPN endpoints. When planning your VPN, you must make a few choices first:

- Will the local end be any device on the LAN, a portion of the local network (as defined by a subnet or by a range of IP addresses), or a single PC?
- Will the remote end be any device on the remote LAN, a portion of the remote network (as defined by a subnet or by a range of IP addresses), or a single PC?
- Will either endpoint use Fully Qualified Domain Names (FQDNs)? Many DSL accounts are provisioned with DHCP addressing, where the IP address of the WAN port can change from time to time. Under these circumstances, configuring the WAN port with a dynamic DNS (DynDNS) service provider simplifies the configuration task. When DynDNS is configured on the WAN port, configure the VPN using FDQN.

FQDNs supplied by Dynamic DNS providers can allow a VPN endpoint with a dynamic IP address to initiate or respond to a tunnel request. Otherwise, the side using a dynamic IP address must always be the initiator.

- What method will you use to configure your VPN tunnels?
  - The VPN Wizard using VPNC defaults (see Table 5-1)
  - Advanced methods (see Chapter 6, "Advanced Virtual Private Networking")

Table 5-1. Parameters recommended by the VPNC and used in the VPN Wizard

Parameter	Factory Default
Secure Association	Main Mode
Authentication Method	Pre-shared Key
Encryption Method	3DES
Authentication Protocol	SHA-1
Diffie-Hellman (DH) Group	Group 2 (1024 bit)
Key Life	8 hours
IKE Life Time	24 hours
NETBIOS	Enabled

- What level of IPSec VPN encryption will you use?
  - DE — The Data Encryption Standard (DES) processes input data that is 64 bits wide, encrypting these values using a 56 bit key. Faster but less secure than 3DES.
  - 3DES — (Triple DES) achieves a higher level of security by encrypting the data three times using DES with three different, unrelated keys.
  - AES
- What level of authentication will you use?
  - MDS — 128 bits, faster but less secure.
  - SHA-1 — 160 bits, slower but more secure.

Note: NETGEAR publishes additional interoperability scenarios with various gateway and client software products.

VPN Tunnel Configuration

There are two tunnel configurations and three ways to configure them:

- Use the VPN Wizard to configure a VPN tunnel (recommended for most situations):
  - See "How to Set Up a Client-to-Gateway VPN Configuration" on page 5-5.
  - See "How to Set Up a Gateway-to-Gateway VPN Configuration" on page 5-20.
- See Chapter 6, "Advanced Virtual Private Networking" when the VPN Wizard and its VPNC defaults (see Table 5-1 on page 5-4) are not appropriate for your special circumstances.

How to Set Up a Client-to-Gateway VPN Configuration

Setting up a VPN between a remote PC running the NETGEAR ProSafe VPN Client and a network gateway (see Figure 5-3) involves the following two steps:

- "Step 1: Configuring the Client-to-Gateway VPN Tunnel on the FVS318v3" on page 5-6 uses the VPN Wizard to configure the VPN tunnel between the remote PC and network gateway.
- "Step 2: Configuring the NETGEAR ProSafe VPN Client on the Remote PC" on page 5-9 configures the NETGEAR ProSafe VPN Client endpoint.

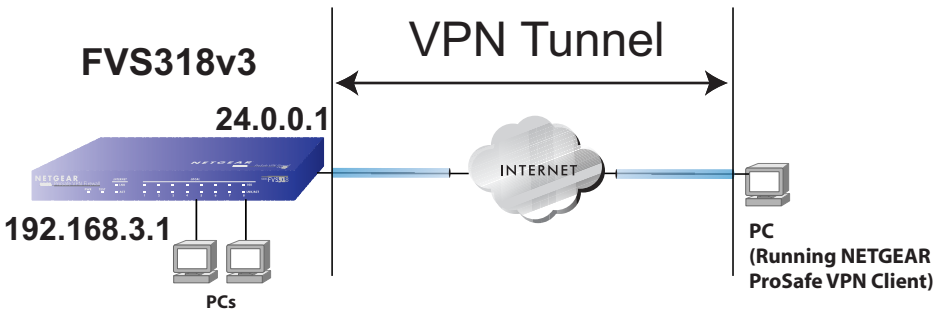


Figure 5-3: Client-to-gateway VPN tunnel

Step 1: Configuring the Client-to-Gateway VPN Tunnel on the FVS318v3

Note: This section uses the VPN Wizard to set up the VPN tunnel using the VPNC default parameters listed in Table 5-1 on page 5-4. If you have special requirements not covered by these VPNC-recommended parameters, refer to Chapter 6, "Advanced Virtual Private Networking" to set up the VPN tunnel.

Follow this procedure to configure a client-to-gateway VPN tunnel using the VPN Wizard.

1. Log in to the FVS318v3 at its LAN address of *http://192.168.0.1* with its default user name of **admin** and password of **password**. Click the **VPN Wizard** link in the main menu to display this screen. Click **Next** to proceed.

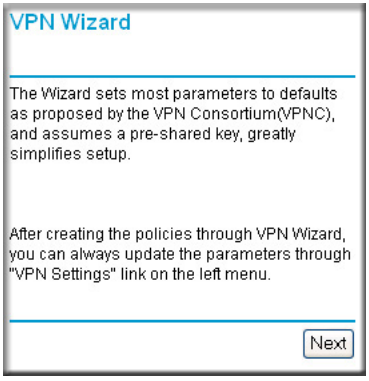

VPN Wizard
The Wizard sets most parameters to defaults as proposed by the VPN Consortium(VPNC), and assumes a pre-shared key, greatly simplifies setup.
After creating the policies through VPN Wizard, you can always update the parameters through "VPN Settings" link on the left menu.
Next

Figure 5-4: VPN Wizard start screen

2. Fill in the Connection Name and the pre-shared key, select the type of target end point, and click **Next** to proceed.

   Note: The Connection Name is arbitrary and not relevant to how the configuration functions.

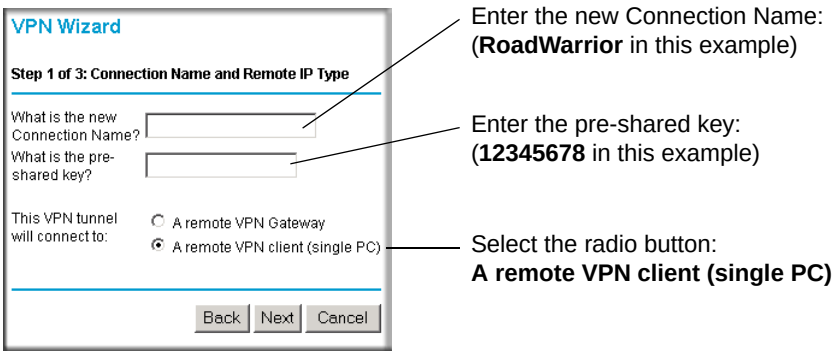

VPN Wizard
Step 1 of 3: Connection Name and Remote IP Type
What is the new Connection Name?
What is the pre-shared key?
This VPN tunnel will connect to:
A remote VPN Gateway
A remote VPN client (single PC)
Back
Next
Cancel
Enter the new Connection Name:
(RoadWarrior in this example)
Enter the pre-shared key:
(12345678 in this example)
Select the radio button:
A remote VPN client (single PC)

Figure 5-5: Connection Name and Remote IP Type

The Summary screen below displays.

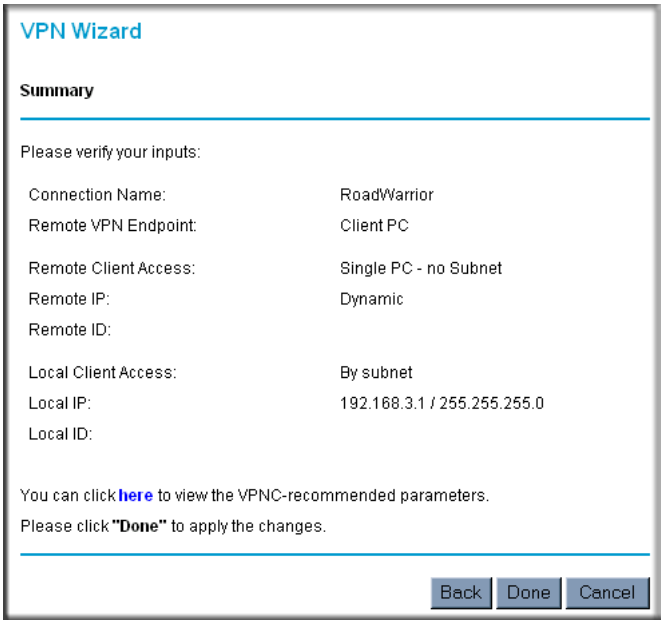


Figure 5-6: VPN Wizard Summary

To view the VPNC recommended authentication and encryption settings used by the VPN Wizard, click the **here** link (see Figure 5-6). Click **Back** to return to the **Summary** screen.

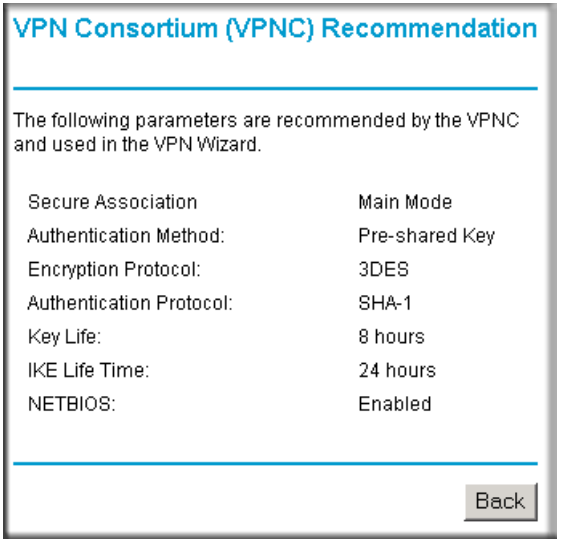


Figure 5-7: VPNC Recommended Settings

3. Click **Done** on the Summary screen (see Figure 5-6) to complete the configuration procedure. The VPN Policies menu below displays showing that the new tunnel is enabled.

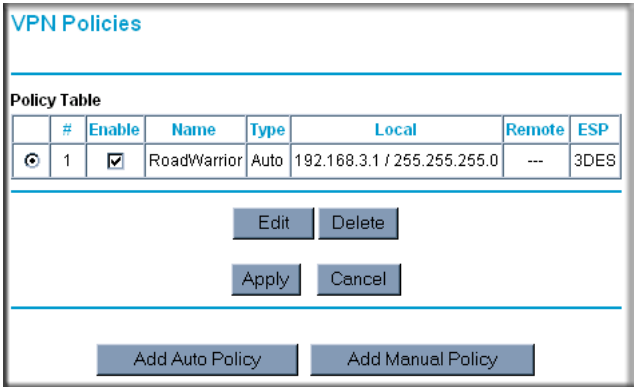


Figure 5-8: VPN Policies

To view or modify the tunnel settings, select the radio button next to the tunnel entry and click **Edit**.

Step 2: Configuring the NETGEAR ProSafe VPN Client on the Remote PC

This procedure describes how to configure the NETGEAR ProSafe VPN Client. This example assumes the PC running the client has a dynamically assigned IP address.

The PC must have the NETGEAR ProSafe VPN Client program installed that supports IPSec. Go to the NETGEAR Web site (*http://www.netgear.com*) and select VPN01L_VPN05L in the Product Quick Find drop-down menu for information on how to purchase the NETGEAR ProSafe VPN Client.

Note: Before installing the NETGEAR ProSafe VPN Client software, be sure to turn off any virus protection or firewall software you may be running on your PC.

1. Install the NETGEAR ProSafe VPN Client on the remote PC and reboot.
   a. You may need to insert your Windows CD to complete the installation.
   b. If you do not have a modem or dial-up adapter installed in your PC, you may see the warning message stating “The NETGEAR ProSafe VPN Component requires at least one dial-up adapter be installed.” You can disregard this message.
   c. Install the IPSec Component. You may have the option to install either the VPN Adapter or the IPSec Component or both. The VPN Adapter is not necessary.
   d. The system should show the ProSafe icon ( ) in the system tray after rebooting.
   e. Double-click the system tray icon to open the Security Policy Editor.
2. Add a new connection.

Note: The procedure in this section explains how to create a new security policy from scratch. For the procedure on how to import an existing security policy that has already been created on another client running the NETGEAR ProSafe VPN Client, see “Transferring a Security Policy to Another Client” on page 5-18.

   a. Run the NETGEAR ProSafe Security Policy Editor program and create a VPN Connection.

b. From the Edit menu of the Security Policy Editor, click **Add**, then **Connection**. A “New Connection” listing appears in the list of policies. Rename the “New Connection” so that it matches the Connection Name you entered in the VPN Settings of the FVS318v3 on LAN A.

Note: In this example, the Connection Name used on the client side of the VPN tunnel is **NETGEAR_VPN_router** and it does not have to match the **RoadWarrior** Connection Name used on the gateway side of the VPN tunnel (see Figure 5-5) because Connection Names are unrelated to how the VPN tunnel functions.

Tip: Choose Connection Names that make sense to the people using and administrating the VPN.

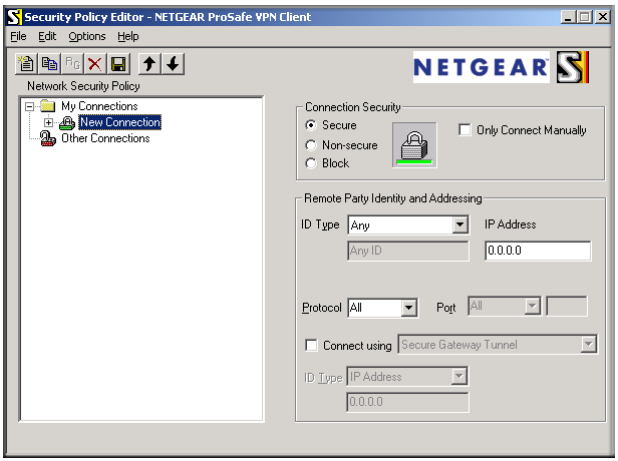


Figure 5-9: Security Policy Editor new connection

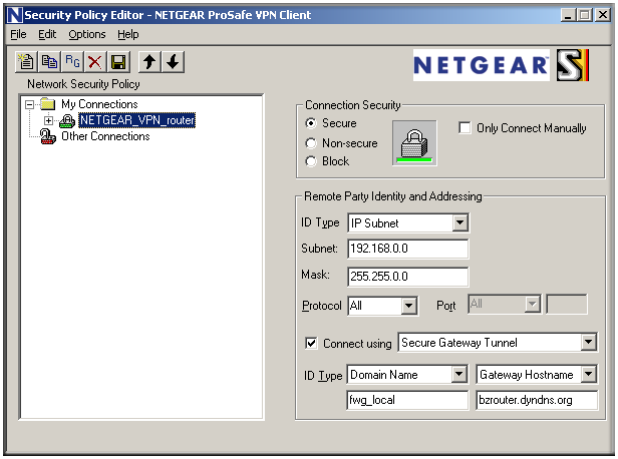


Figure 5-10: Security Policy Editor connection settings

c. Select Secure in the Connection Security check box.

d. Select IP Subnet in the ID Type menu.

In this example, type **192.168.3.1** in the Subnet field as the network address of the FVS318v3.

e. Enter **255.255.255.0** in the Mask field as the LAN Subnet Mask of the FVS318v3.

f. Select All in the Protocol menu to allow all traffic through the VPN tunnel.

g. Select the Connect using Secure Gateway Tunnel check box.

h. Select IP Address in the ID Type menu below the check box.

i. Enter the public WAN IP Address of the FVS318v3 in the field directly below the ID Type menu. In this example, **22.23.24.25** would be used.

The resulting Connection Settings are shown in Figure 5-10.

3. Configure the Security Policy in the NETGEAR ProSafe VPN Client software.

a. In the Network Security Policy list, expand the new connection by double clicking its name or clicking on the “+” symbol. My Identity and Security Policy subheadings appear below the connection name.

b. Click on the **Security Policy** subheading to show the Security Policy menu.

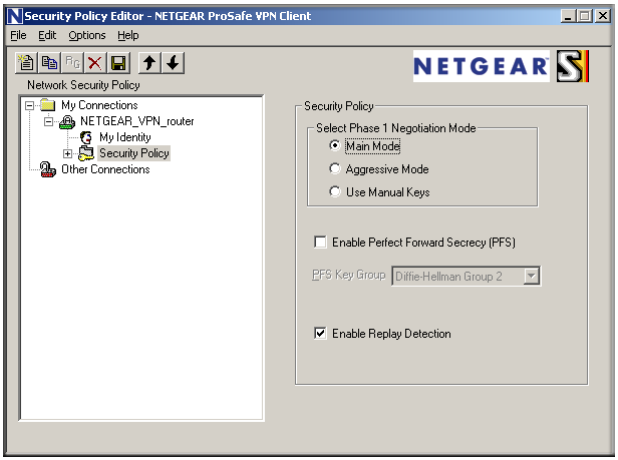


Figure 5-11: Security Policy Editor Security Policy

c. Select the Main Mode in the Select Phase 1 Negotiation Mode check box.

4. Configure the VPN Client Identity.

   In this step, you will provide information about the remote VPN client PC. You will need to provide:

   — The Pre-Shared Key that you configured in the FVS318v3.

   — Either a fixed IP address or a “fixed virtual” IP address of the VPN client PC.

   a. In the Network Security Policy list on the left side of the Security Policy Editor window, click on **My Identity**.

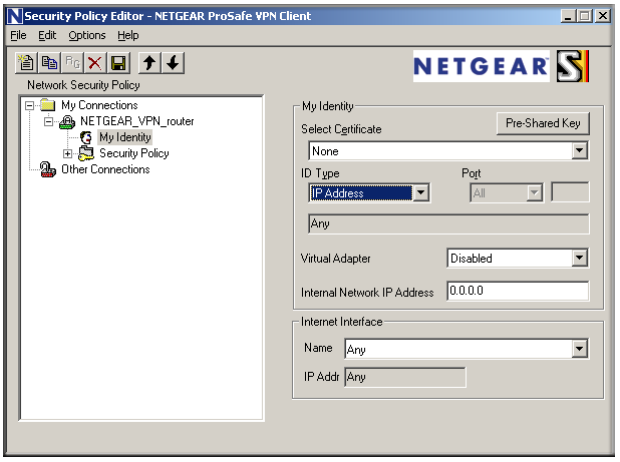


Figure 5-12: Security Policy Editor My Identity

b. Choose None in the Select Certificate box.

c. Select IP Address in the ID Type box. If you are using a virtual fixed IP address, enter this address in the Internal Network IP Address box. Otherwise, leave this box empty.

d. In the Internet Interface box, select the adapter you use to access the Internet. Select PPP Adapter in the Name menu if you have a dial-up Internet account. Select your Ethernet adapter if you have a dedicated Cable or DSL line. You may also choose Any if you will be switching between adapters or if you have only one adapter.

e. Click the **Pre-Shared Key** button. In the Pre-Shared Key dialog box, click the **Enter Key** button. Enter the FVS318v3's Pre-Shared Key and click **OK**. In this example, **12345678** is entered. This field is case sensitive.

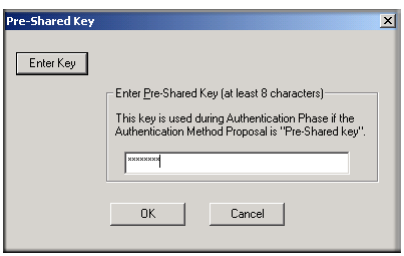

Pre-Shared Key
Enter Key
Enter Pre-Shared Key (at least 8 characters)
This key is used during Authentication Phase if the Authentication Method Proposal is "Pre-Shared key".
OK
Cancel

Figure 5-13: Security Policy Editor Pre-Shared Key

5. Configure the VPN Client Authentication Proposal.

   In this step, you will provide the type of encryption (DES or 3DES) to be used for this connection. This selection must match your selection in the FVS318v3 configuration.

   a. In the Network Security Policy list on the left side of the Security Policy Editor window, expand the Security Policy heading by double clicking its name or clicking on the "+" symbol.

   b. Expand the Authentication subheading by double clicking its name or clicking on the "+" symbol. Then select Proposal 1 below Authentication.

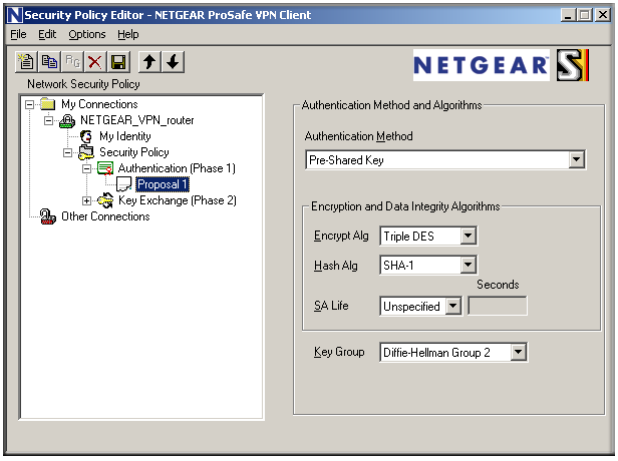


Figure 5-14: Security Policy Editor Authentication

   c. In the Authentication Method menu, select Pre-Shared key.

   d. In the Encrypt Alg menu, select the type of encryption. In this example, use Triple DES.

   e. In the Hash Alg menu, select SHA-1.

   f. In the SA Life menu, select Unspecified.

   g. In the Key Group menu, select Diffie-Hellman Group 2.

6. Configure the VPN Client Key Exchange Proposal.

   In this step, you will provide the type of encryption (DES or 3DES) to be used for this connection. This selection must match your selection in the FVS318v3 configuration.

   a. Expand the Key Exchange subheading by double clicking its name or clicking on the "+" symbol. Then select Proposal 1 below Key Exchange.

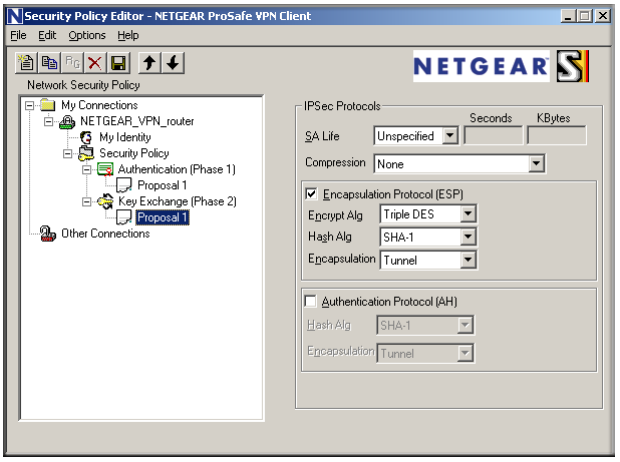


Figure 5-15: Security Policy Editor Key Exchange

b. In the SA Life menu, select Unspecified.

c. In the Compression menu, select None.

d. Check the Encapsulation Protocol (ESP) check box.

e. In the Encrypt Alg menu, select the type of encryption. In this example, use Triple DES.

f. In the Hash Alg menu, select SHA-1.

g. In the Encapsulation menu, select Tunnel.

h. Leave the Authentication Protocol (AH) check box unchecked.

7. Save the VPN Client Settings.

   From the File menu at the top of the Security Policy Editor window, select Save.

   After you have configured and saved the VPN client information, your PC will automatically open the VPN connection when you attempt to access any IP addresses in the range of the remote VPN firewall's LAN.

8. Check the VPN Connection.

   To check the VPN Connection, you can initiate a request from the remote PC to the FVS318v3's network by using the "Connect" option in the NETGEAR ProSafe menu bar. The NETGEAR ProSafe client will report the results of the attempt to connect. Since the remote PC has a dynamically assigned WAN IP address, it must initiate the request.

   To perform a ping test using our example, start from the remote PC:

a. Establish an Internet connection from the PC.

b. On the Windows taskbar, click the **Start** button, and then click **Run**.

c. Type **`ping -t 192.168.3.1`** , and then click **OK**.

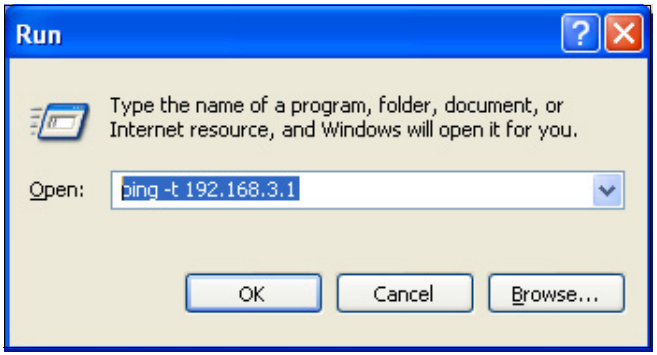


Figure 5-16: Running a Ping test to the LAN from the PC

This will cause a continuous ping to be sent to the first FVS318v3. After between several seconds and two minutes, the ping response should change from “timed out” to “reply.”

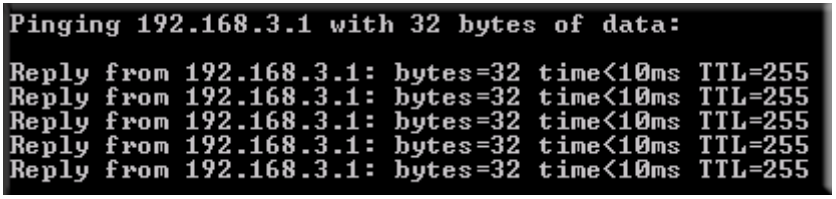

Pinging 192.168.3.1 with 32 bytes of data:
Reply from 192.168.3.1: bytes=32 time<10ms TTL=255
Reply from 192.168.3.1: bytes=32 time<10ms TTL=255
Reply from 192.168.3.1: bytes=32 time<10ms TTL=255
Reply from 192.168.3.1: bytes=32 time<10ms TTL=255
Reply from 192.168.3.1: bytes=32 time<10ms TTL=255

Figure 5-17: Ping test results

Once the connection is established, you can open the browser of the PC and enter the LAN IP address of the remote FVS318v3. After a short wait, you should see the login screen of the VPN Firewall (unless another PC already has the FVS318v3 management interface open).

Monitoring the Progress and Status of the VPN Client Connection

Information on the progress and status of the VPN client connection can be viewed by opening the NETGEAR ProSafe Log Viewer.

1. To launch this function, click on the **Windows Start** button, then select **Programs**, then **NETGEAR ProSafe VPN Client**, then **Log Viewer**.

The Log Viewer screen for a similar successful connection is shown below:

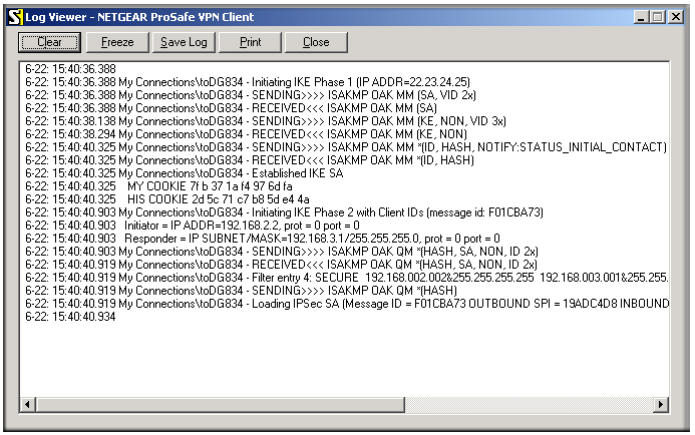

Log Viewer - NETGEAR ProSafe VPN Client
Clear
Freeze
Save Log
Print
Close
6-22: 15:40:36.388
6-22: 15:40:36.388 My Connections\toDG834 - Initiating IKE Phase 1 (IP ADDR=22.23.24.25)
6-22: 15:40:36.388 My Connections\toDG834 - SENDING>>>> ISAKMP OAK MM (SA, VID 2x)
6-22: 15:40:36.388 My Connections\toDG834 - RECEIVED<<< ISAKMP OAK MM (SA)
6-22: 15:40:38.138 My Connections\toDG834 - SENDING>>>> ISAKMP OAK MM (KE, NON, VID 3x)
6-22: 15:40:38.294 My Connections\toDG834 - RECEIVED<<< ISAKMP OAK MM (KE, NON)
6-22: 15:40:40.325 My Connections\toDG834 - SENDING>>>> ISAKMP OAK MM *(ID, HASH, NOTIFY:STATUS_INITIAL_CONTACT)
6-22: 15:40:40.325 My Connections\toDG834 - RECEIVED<<< ISAKMP OAK MM *(ID, HASH)
6-22: 15:40:40.325 My Connections\toDG834 - Established IKE SA
6-22: 15:40:40.325 MY COOKIE 7f b 37 1a f4 97 6d fa
6-22: 15:40:40.325 HIS COOKIE 2d 5c 71 c7 b8 5d e4 4a
6-22: 15:40:40.903 My Connections\toDG834 - Initiating IKE Phase 2 with Client IDs (message id: F01CBA73)
6-22: 15:40:40.903 Initiator = IP ADDR=192.168.2.2, prot = 0 port = 0
6-22: 15:40:40.903 Responder = IP SUBNET/MASK=192.168.3.1/255.255.255.0, prot = 0 port = 0
6-22: 15:40:40.903 My Connections\toDG834 - SENDING>>>> ISAKMP OAK QM *(HASH, SA, NON, ID 2x)
6-22: 15:40:40.919 My Connections\toDG834 - RECEIVED<<< ISAKMP OAK QM *(HASH, SA, NON, ID 2x)
6-22: 15:40:40.919 My Connections\toDG834 - Filter entry 4: SECURE 192.168.002.002&255.255.255.255 192.168.003.001&255.255.
6-22: 15:40:40.919 My Connections\toDG834 - SENDING>>>> ISAKMP OAK QM *(HASH)
6-22: 15:40:40.919 My Connections\toDG834 - Loading IPSec SA (Message ID = F01CBA73 OUTBOUND SPI = 19ADC4D8 INBOUND
6-22: 15:40:40.934

Figure 5-18: Log Viewer screen

	Note: Use the active VPN tunnel information and pings to determine whether a failed connection is due to the VPN tunnel or some reason outside the VPN tunnel.

2. The Connection Monitor screen for a similar connection is shown below:

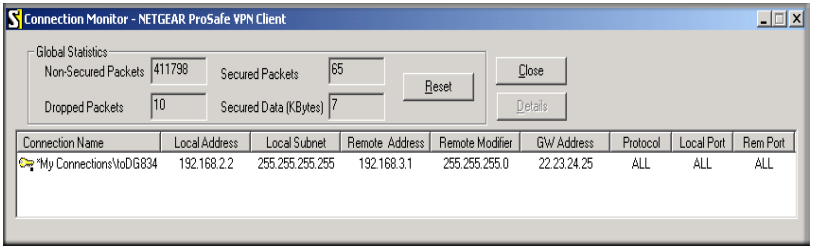


Figure 5-19: Connection Monitor screen

In this example you can see the following:

- The FVS318v3 has a public IP WAN address of 22.23.24.25.
- The FVS318v3 has a LAN IP address of 192.168.3.1.
- The VPN client PC has a dynamically assigned address of 192.168.2.2.

While the connection is being established, the Connection Name field in this menu will say “SA” before the name of the connection. When the connection is successful, the “SA” will change to the yellow key symbol shown in the illustration above.

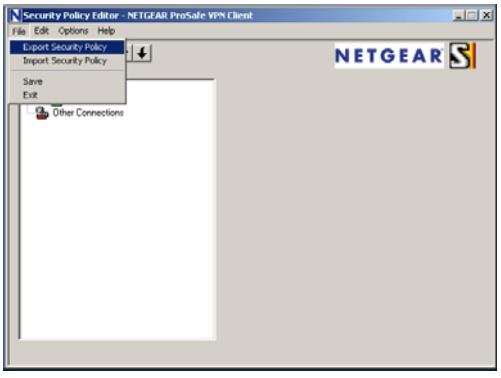
Note: While your PC is connected to a remote LAN through a VPN, you might not have normal Internet access. If this is the case, you will need to close the VPN connection in order to have normal Internet access.

Transferring a Security Policy to Another Client

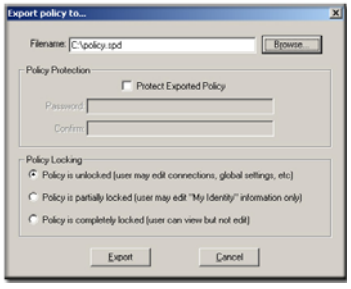
This section explains how to export and import a security policy as an **.spd** file so that an existing NETGEAR ProSafe VPN Client configuration can be copied to other PCs running the NETGEAR ProSafe VPN Client.

Exporting a Security Policy

The following procedure (Figure 5-20) enables you to export a security policy as an **.spd** file.



Step 1: Select **Export Security Policy** from the **File** pulldown.



Step 2: Click **Export** once you decide the name of the file and directory where you want to store the client policy.

In this example, the exported policy is named **policy.spd** and is being stored on the C drive.

Figure 5-20: Exporting a security policy

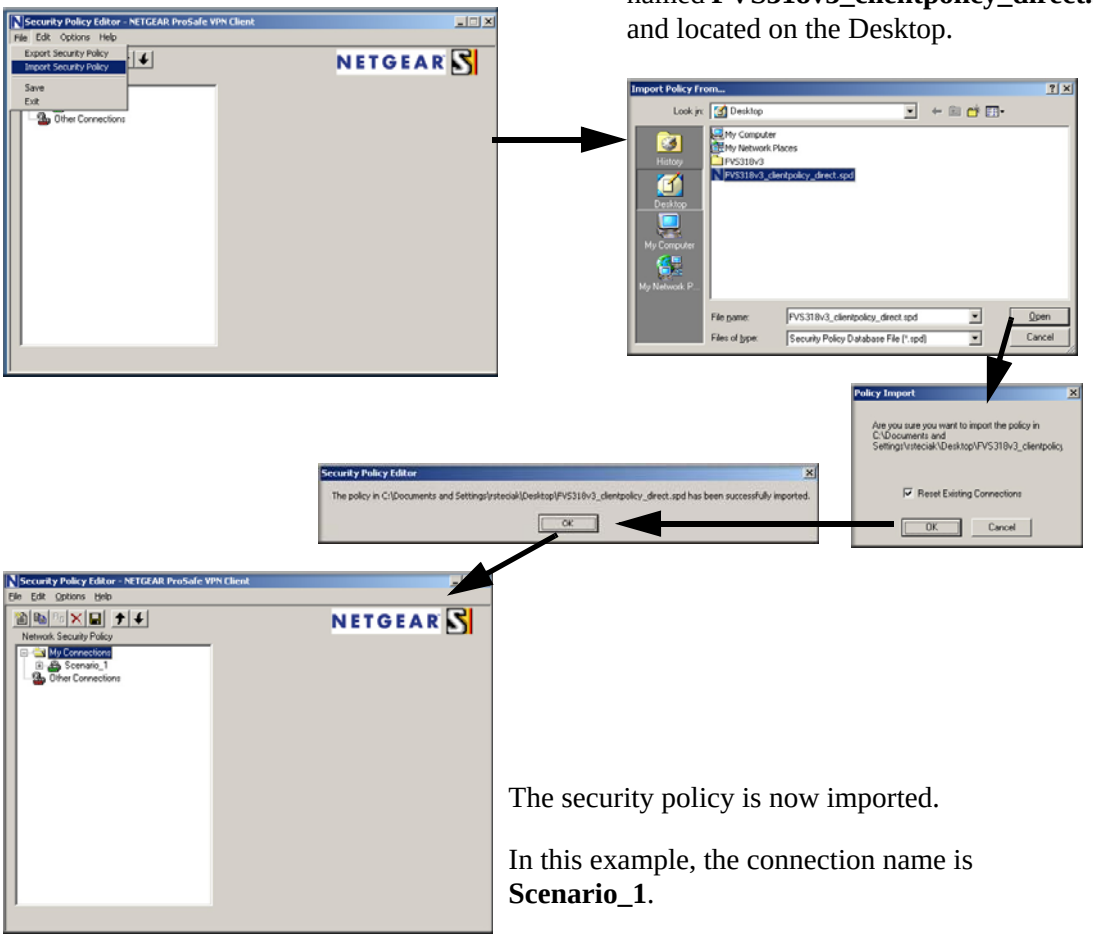
Importing a Security Policy

The following procedure (Figure 5-21) enables you to import an existing security policy.

Step 1: Invoke the NETGEAR ProSafe VPN Client and select **Import Security Policy** from the **File** pulldown.

Step 2: Select the security policy to import.

In this example, the security policy file is named **FVS318v3_clientpolicy_direct.spd** and located on the Desktop.



The security policy is now imported.

In this example, the connection name is **Scenario_1**.

Figure 5-21: Importing a security policy

How to Set Up a Gateway-to-Gateway VPN Configuration

Note: This section uses the VPN Wizard to set up the VPN tunnel using the VPNC default parameters listed in Table 5-1 on page 5-4. If you have special requirements not covered by these VPNC-recommended parameters, refer to Chapter 6, "Advanced Virtual Private Networking" to set up the VPN tunnel.

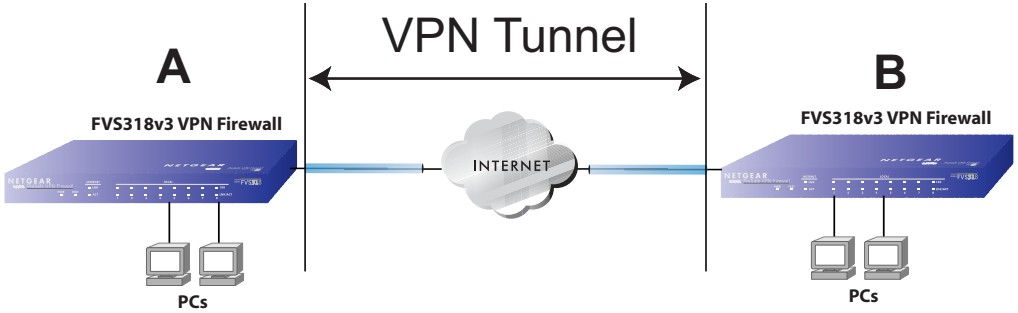


Figure 5-22: Gateway-to-Gateway VPN Tunnel

Follow the procedure below to set the LAN IPs on each FVS318v3 to different subnets and configure each properly for the Internet.

The LAN IP address ranges of each VPN endpoint must be different. The connection will fail if both are using the NETGEAR default address range of 192.168.0.x.

In this example, LAN A uses 192.168.0.1 and LAN B uses 192.168.3.1.

Procedure to Configure a Gateway-to-Gateway VPN Tunnel

Follow this procedure to configure a gateway-to-gateway VPN tunnel using the VPN Wizard.

1. Log in to the FVS318v3 on LAN A at its default LAN address of *http://192.168.0.1* with its default user name of **admin** and password of **password**. Click the **VPN Wizard** link in the main menu to display this screen. Click **Next** to proceed.

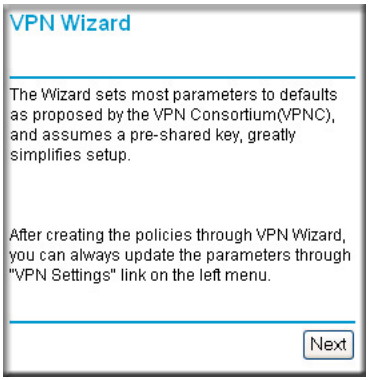

VPN Wizard
The Wizard sets most parameters to defaults as proposed by the VPN Consortium(VPNC), and assumes a pre-shared key, greatly simplifies setup.
After creating the policies through VPN Wizard, you can always update the parameters through "VPN Settings" link on the left menu.
Next

Figure 5-23: VPN Wizard start screen

2. Fill in the Connection Name and the pre-shared key, select the type of target end point, and click **Next** to proceed.

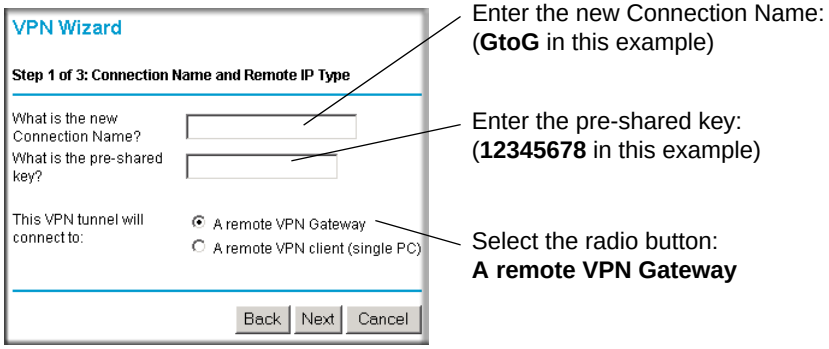
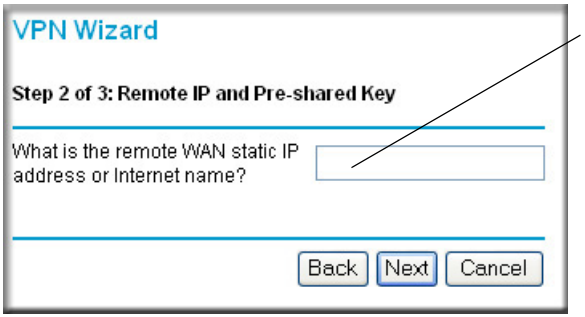

VPN Wizard
Step 1 of 3: Connection Name and Remote IP Type
What is the new Connection Name?
What is the pre-shared key?
This VPN tunnel will connect to:
A remote VPN Gateway
A remote VPN client (single PC)
Back
Next
Cancel
Enter the new Connection Name: (GtoG in this example)
Enter the pre-shared key: (12345678 in this example)
Select the radio button: A remote VPN Gateway

Figure 5-24: Connection Name and Remote IP Type

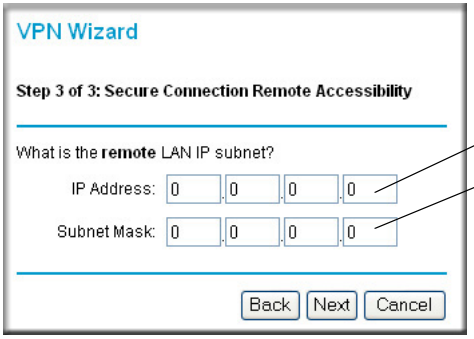
3. Fill in the IP Address or FQDN for the target VPN endpoint WAN connection and click **Next**.


VPN Wizard
Step 2 of 3: Remote IP and Pre-shared Key
What is the remote WAN static IP address or Internet name?
Back
Next
Cancel

Enter the WAN IP address of the remote VPN gateway:
(**22.23.24.25** in this example)

Figure 5-25: Remote IP

4. Identify the IP addresses at the target endpoint that can use this tunnel, and click **Next**.


VPN Wizard
Step 3 of 3: Secure Connection Remote Accessibility
What is the remote LAN IP subnet?
IP Address: 0 0 0 0
Subnet Mask: 0 0 0 0
Back
Next
Cancel

Enter the LAN IP settings of the remote VPN gateway:
- IP Address
  (**192.168.3.1** in this example)
- Subnet Mask
  (**255.255.255.0** in this example)

Figure 5-26: Secure Connection Remote Accessibility

The Summary screen below displays.

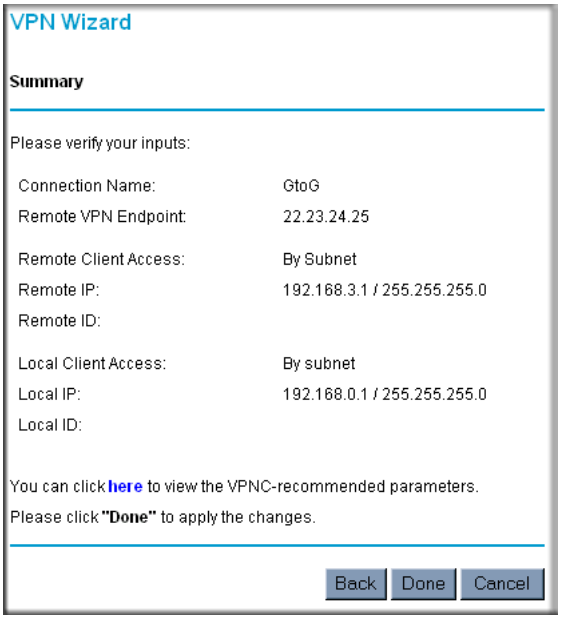


Figure 5-27: VPN Wizard Summary

To view the VPNC recommended authentication and encryption settings used by the VPN Wizard, click the **here** link (see Figure 5-27). Click **Back** to return to the Summary screen.

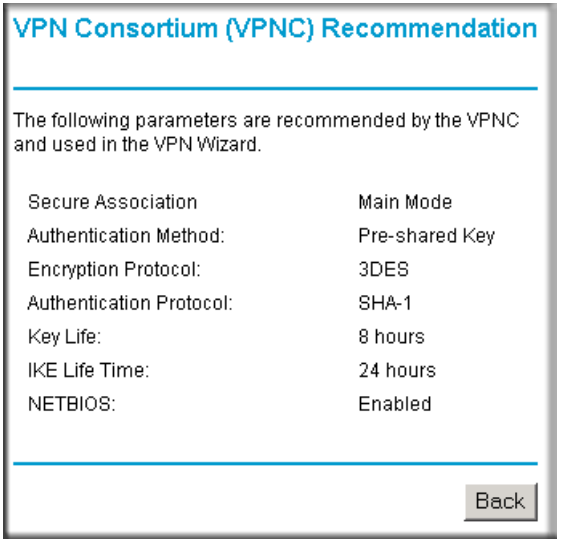


Figure 5-28: VPN Recommended Settings

5. Click **Done** on the Summary screen (see Figure 5-27) to complete the configuration procedure. The VPN Policies menu below displays showing that the new tunnel is enabled.

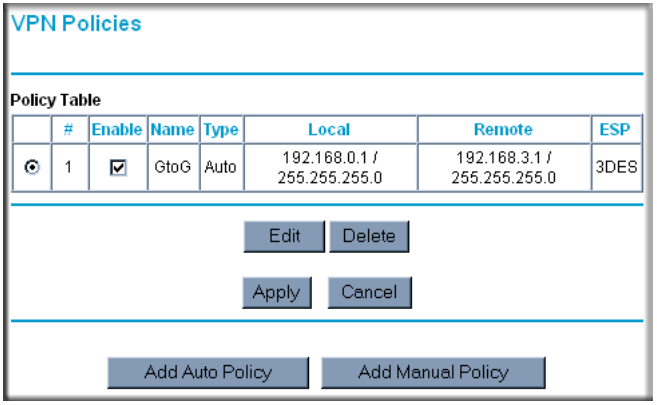


Figure 5-29: VPN Policies

6. Repeat for the FVS318v3 on LAN B. Pay special attention and use the following network settings as appropriate.
   - WAN IP of the remote VPN gateway (e.g., **14.15.16.17**)
   - LAN IP settings of the remote VPN gateway:
     — IP Address (e.g, **192.168.0.1**)
     — Subnet Mask (e.g., **255.255.255.0**)
     — Preshared Key (e.g., **12345678**)
7. Use the VPN Status screen to activate the VPN tunnel by performing the following steps:

Note: The VPN Status screen is only one of three ways to active a VPN tunnel. See "Activating a VPN Tunnel" on page 5-26 for information on the other ways.

a. Open the FVS318v3 management interface and click on **VPN Status** under VPN to get the VPN Status/Log screen (Figure 5-30).

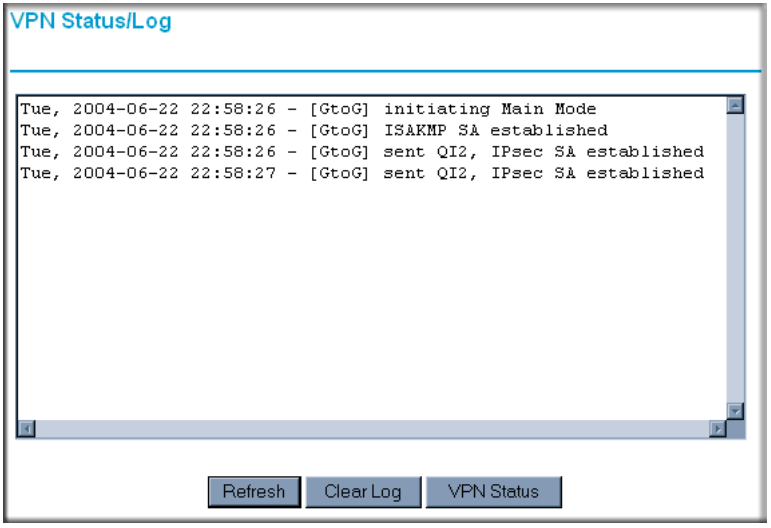

VPN Status/Log
Tue, 2004-06-22 22:58:26 - [GtoG] initiating Main Mode
Tue, 2004-06-22 22:58:26 - [GtoG] ISAKMP SA established
Tue, 2004-06-22 22:58:26 - [GtoG] sent QI2, IPsec SA established
Tue, 2004-06-22 22:58:27 - [GtoG] sent QI2, IPsec SA established
Refresh
Clear Log
VPN Status

Figure 5-30: VPN Status/Log screen

b. Click on **VPN Status** (Figure 5-32) to get the Current VPN Tunnels (SAs) screen (Figure 5-31). Click on **Connect** for the VPN tunnel you want to activate.

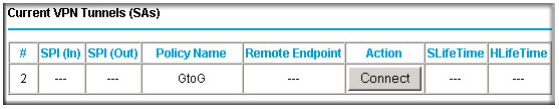


Figure 5-31: Current VPN Tunnels (SAs) Screen

c. Look at the VPN Status/Log screen (Figure 5-30) to verify that the tunnel is connected.

VPN Tunnel Control

Activating a VPN Tunnel

There are three ways to activate a VPN tunnel:

- Start using the VPN tunnel.
- Use the VPN Status page.
- Activate the VPN tunnel by pinging the remote endpoint.

Start Using a VPN Tunnel to Activate It

To use a VPN tunnel, use a Web browser to go to a URL whose IP address or range is covered by the policy for that VPN tunnel.

Using the VPN Status Page to Activate a VPN Tunnel

To use the VPN Status screen to activate a VPN tunnel, perform the following steps:

1. Log in to the VPN Firewall.
2. Open the FVS318v3 management interface and click on **VPN Status** under VPN to get the VPN Status/Log screen (Figure 5-32).

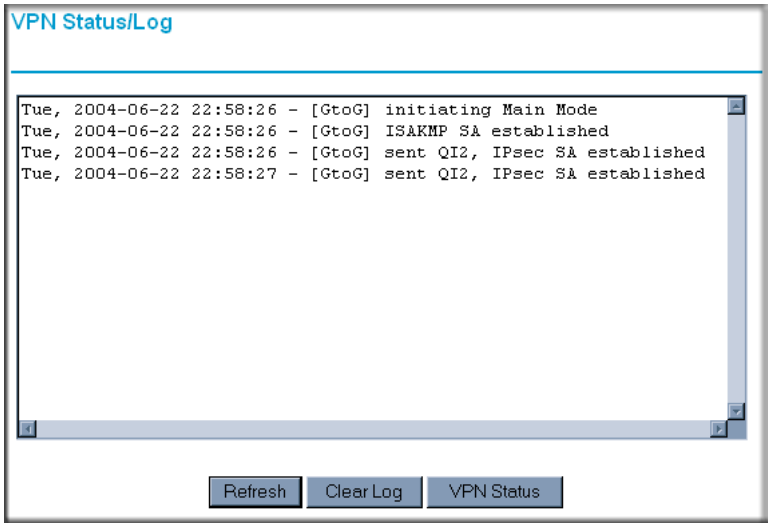

VPN Status/Log
Tue, 2004-06-22 22:58:26 - [GtoG] initiating Main Mode
Tue, 2004-06-22 22:58:26 - [GtoG] ISAKMP SA established
Tue, 2004-06-22 22:58:26 - [GtoG] sent QI2, IPsec SA established
Tue, 2004-06-22 22:58:27 - [GtoG] sent QI2, IPsec SA established
Refresh
Clear Log
VPN Status

Figure 5-32: VPN Status/Log screen

3. Click **VPN Status** (Figure 5-32) to get the Current VPN Tunnels (SAs) screen (Figure 5-33). Click **Connect** for the VPN tunnel you want to activate.

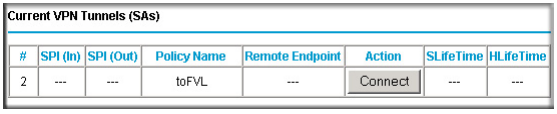


Figure 5-33: Current VPN Tunnels (SAs) screen

Activate the VPN Tunnel by Pinging the Remote Endpoint

Note: This section uses 192.168.3.1 for an example remote endpoint LAN IP address.

To activate the VPN tunnel by pinging the remote endpoint (192.168.3.1), do the following steps depending on whether your configuration is client-to-gateway or gateway-to-gateway:

- **Client-to-Gateway Configuration**—to check the VPN Connection, you can initiate a request from the remote PC to the FVS318v3's network by using the "Connect" option in the NETGEAR ProSafe menu bar. The NETGEAR ProSafe client will report the results of the attempt to connect. Since the remote PC has a dynamically assigned WAN IP address, it must initiate the request.

  To perform a ping test using our example, start from the remote PC:

a. Establish an Internet connection from the PC.

b. On the Windows taskbar, click the **Start** button, and then click **Run**.

c. Type **ping -t 192.168.3.1** and then click **OK**.

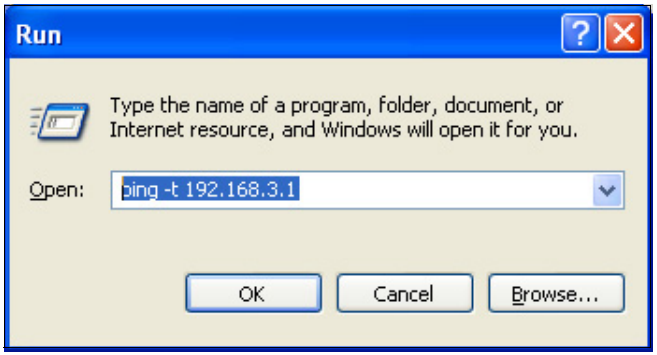


Figure 5-34: Running a Ping test to the LAN from the PC

This will cause a continuous ping to be sent to the first FVS318v3. Within two minutes, the ping response should change from "timed out" to "reply."

Note: Use **Ctrl-C** to stop the pinging.

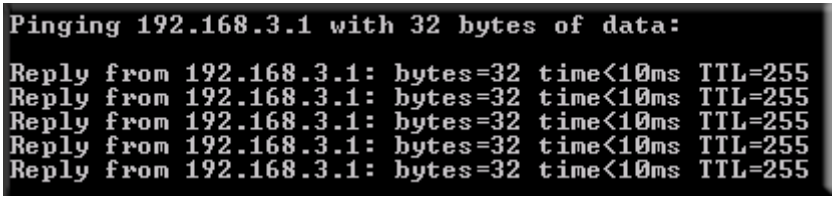

Pinging 192.168.3.1 with 32 bytes of data:
Reply from 192.168.3.1: bytes=32 time<10ms TTL=255
Reply from 192.168.3.1: bytes=32 time<10ms TTL=255
Reply from 192.168.3.1: bytes=32 time<10ms TTL=255
Reply from 192.168.3.1: bytes=32 time<10ms TTL=255
Reply from 192.168.3.1: bytes=32 time<10ms TTL=255

Figure 5-35: Ping test results

Once the connection is established, you can open the browser of the PC and enter the LAN IP address of the remote FVS318v3. After a short wait, you should see the login screen of the VPN Firewall (unless another PC already has the FVS318v3 management interface open).

- **Gateway-to-Gateway Configuration**—test the VPN tunnel by pinging the remote network from a PC attached to the FVS318v3.

  a. Open a command prompt (**Start** -> **Run** -> **cmd**).

  b. Type **ping 192.168.3.1**.

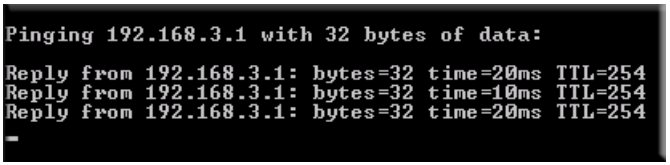

Pinging 192.168.3.1 with 32 bytes of data:
Reply from 192.168.3.1: bytes=32 time=20ms TTL=254
Reply from 192.168.3.1: bytes=32 time=10ms TTL=254
Reply from 192.168.3.1: bytes=32 time=20ms TTL=254

Figure 5-36: Pinging test results

Note: The pings may fail the first time. If so, then try the pings a second time.

Verifying the Status of a VPN Tunnel

To use the VPN Status page to determine the status of a VPN tunnel, perform the following steps:

1. Log in to the VPN Firewall.
2. Open the FVS318v3 management interface and click **VPN Status** under VPN to get the VPN Status/Log screen (Figure 5-37).

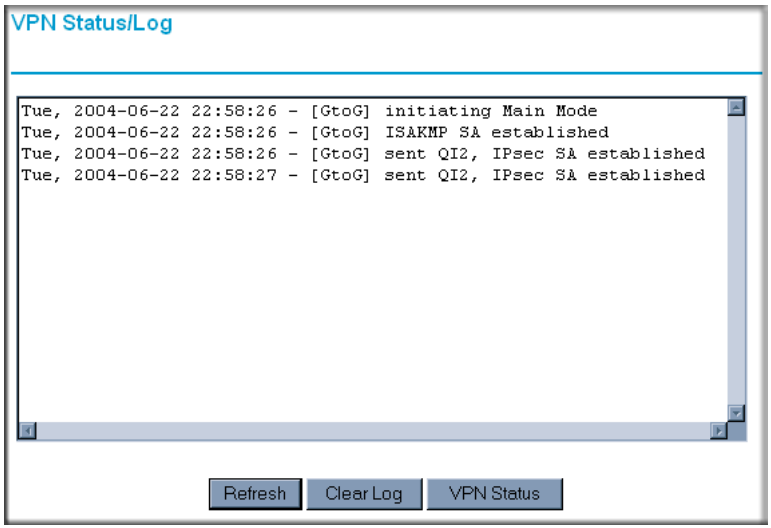

VPN Status/Log
Tue, 2004-06-22 22:58:26 - [GtoG] initiating Main Mode
Tue, 2004-06-22 22:58:26 - [GtoG] ISAKMP SA established
Tue, 2004-06-22 22:58:26 - [GtoG] sent QI2, IPsec SA established
Tue, 2004-06-22 22:58:27 - [GtoG] sent QI2, IPsec SA established
Refresh
Clear Log
VPN Status

Figure 5-37: VPN Status/Log screen

Log—this log shows the details of recent VPN activity, including the building of the VPN tunnel. If there is a problem with the VPN tunnel, refer to the log for information about what might be the cause of the problem.

- Click **Refresh** to see the most recent entries.

- Click **Clear Log** to delete all log entries.

3. Click **VPN Status** (Figure 5-37) to get the Current VPN Tunnels (SAs) screen (Figure 5-38).

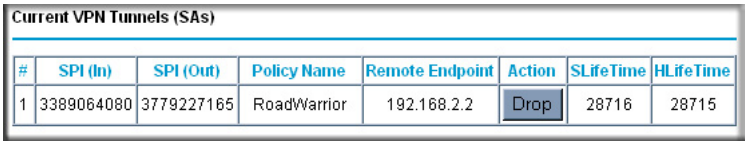

Current VPN Tunnels (SAs)
SPI (In) SPI (Out) Policy Name Remote Endpoint Action SLifeTime HLifeTime
1 3389064080 3779227165 RoadWarrior 192.168.2.2 Drop 28716 28715

Figure 5-38: Current VPN Tunnels (SAs) screen

This page lists the following data for each active VPN Tunnel.

- **SPI**—each SA has a unique SPI (Security Parameter Index) for traffic in each direction. For Manual key exchange, the SPI is specified in the Policy definition. For Automatic key exchange, the SPI is generated by the IKE protocol.
- **Policy Name**—the name of the VPN policy associated with this SA.
- **Remote Endpoint**—the IP address on the remote VPN Endpoint.
- **Action**—the action will be either a **Drop** or a **Connect** button.
- **SLifeTime (Secs)**—the remaining Soft Lifetime for this SA in seconds. When the Soft Lifetime becomes zero, the SA (Security Association) will re-negotiated.
- **HLifeTime (Secs)**—the remaining Hard Lifetime for this SA in seconds. When the Hard Lifetime becomes zero, the SA (Security Association) will be terminated. (It will be re-established if required.)

Deactivating a VPN Tunnel

Sometimes a VPN tunnel must be deactivated for testing purposes. There are two ways to deactivate a VPN tunnel:

- Policy table on VPN Policies page
- VPN Status page

Using the Policy Table on the VPN Policies Page to Deactivate a VPN Tunnel

To use the VPN Policies page to deactivate a VPN tunnel, perform the following steps:

1. Log in to the VPN Firewall.
2. Click on **VPN Policies** under VPN to get the VPN Policies screen below (Figure 5-39).

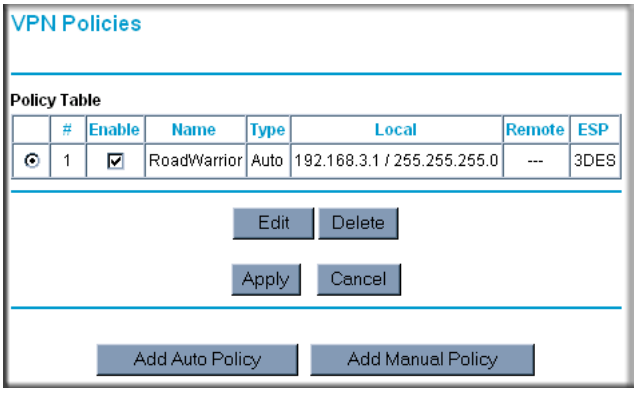


Figure 5-39: VPN Policies

3. Clear the Enable check box for the VPN tunnel you want to deactivate and click **Apply**. (To reactivate the tunnel, check the Enable box and click **Apply**.)

Using the VPN Status Page to Deactivate a VPN Tunnel

To use the VPN Status page to deactivate a VPN tunnel, perform the following steps:

1. Log in to the VPN Firewall.
2. Click **VPN Status** under VPN to get the VPN Status/Log screen (Figure 5-40).

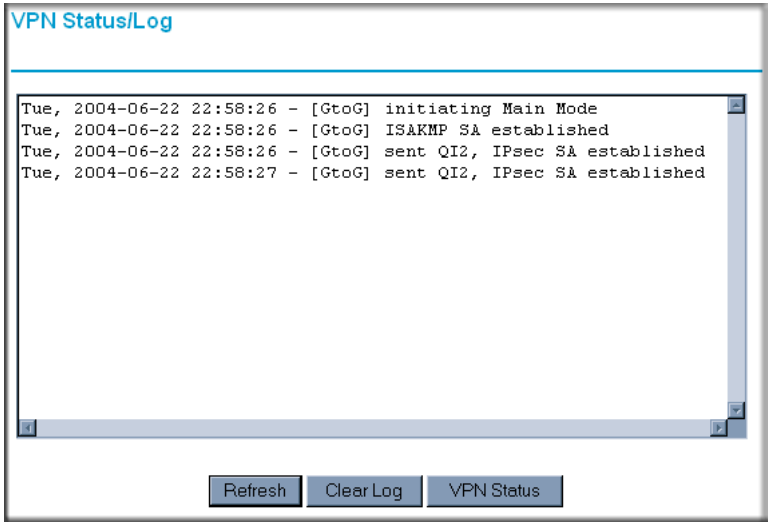

VPN Status/Log
Tue, 2004-06-22 22:58:26 - [GtoG] initiating Main Mode
Tue, 2004-06-22 22:58:26 - [GtoG] ISAKMP SA established
Tue, 2004-06-22 22:58:26 - [GtoG] sent QI2, IPsec SA established
Tue, 2004-06-22 22:58:27 - [GtoG] sent QI2, IPsec SA established
Refresh
Clear Log
VPN Status

Figure 5-40: VPN Status/Log screen

3. Click **VPN Status** (Figure 5-40) to get the Current VPN Tunnels (SAs) screen (Figure 5-41). Click **Drop** for the VPN tunnel you want to deactivate.

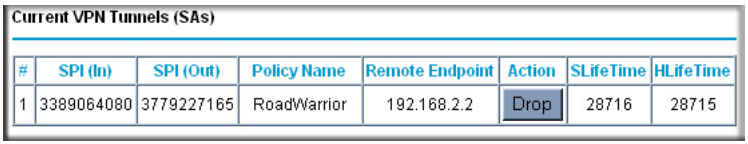

Current VPN Tunnels (SAs)
SPI (In) SPI (Out) Policy Name Remote Endpoint Action SLifeTime HLifeTime
1 3389064080 3779227165 RoadWarrior 192.168.2.2 Drop 28716 28715

Figure 5-41: Current VPN Tunnels (SAs) screen

Note: When NETBIOS is enabled (which it is in the VPNC defaults implemented by the VPN Wizard), automatic traffic will reactivate the tunnel. To prevent reactivation from happening, either disable NETBIOS or disable the policy for the tunnel (see "Using the Policy Table on the VPN Policies Page to Deactivate a VPN Tunnel" on page 5-30).

Deleting a VPN Tunnel

To delete a VPN tunnel:

1. Log in to the VPN Firewall.
2. Click **VPN Policies** under VPN to display the VPN Policies screen (Figure 5-42). Select the radio button for the VPN tunnel to be deleted and click the **Delete** button.

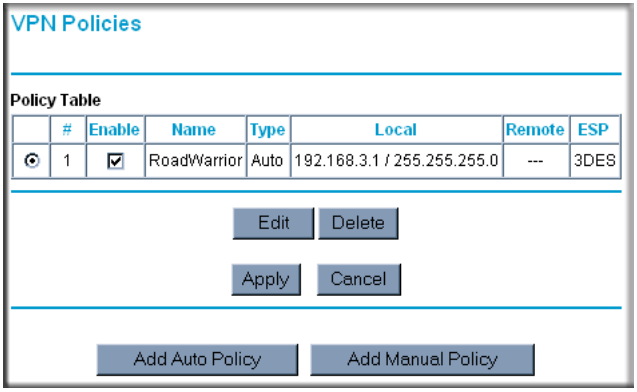

VPN Policies
Policy Table
Enable Name Type Local Remote ESP
1 RoadWarrior Auto 192.168.3.1 / 255.255.255.0 --- 3DES
Edit Delete
Apply Cancel
Add Auto Policy Add Manual Policy

Figure 5-42: VPN Policies

Chapter 6
Advanced Virtual Private Networking

This chapter describes how to use the advanced virtual private networking (VPN) features of the FVS318v3 VPN Firewall. See Chapter 5, “Basic Virtual Private Networking” for a description on how to use the basic VPN features.

Overview of FVS318v3 Policy-Based VPN Configuration

The FVS318v3 uses state-of-the-art firewall and security technology to facilitate controlled and actively monitored VPN connectivity. Since the FVS318v3 strictly conforms to IETF standards, it is interoperable with devices from major network equipment vendors.

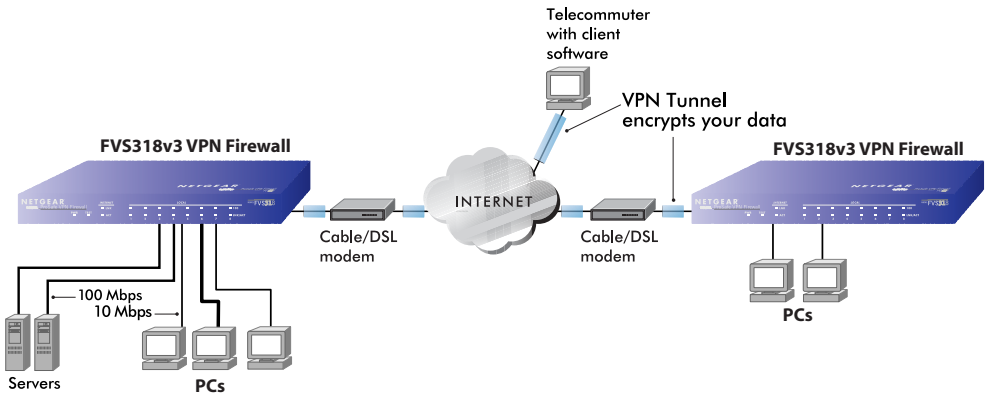


Figure 6-1: Secure access through FVS318v3 VPN firewalls

Using Policies to Manage VPN Traffic

You create policy definitions to manage VPN traffic on the FVS318v3. There are two kinds of policies:

- **IKE Policies**: Define the authentication scheme and automatically generate the encryption keys. As an alternative option, to further automate the process, you can create an IKE policy that uses a trusted certificate authority to provide the authentication while the IKE policy still handles the encryption.
- **VPN Policies**: Apply the IKE policy to specific traffic that requires a VPN tunnel. Or, you can create a VPN policy that does not use an IKE policy but in which you manually enter all the authentication and key parameters.

Since VPN policies use IKE policies, you define the IKE policy first. The FVS318v3 also allows you to manually input the authentication scheme and encryption key values. In the case of manual key management there will not be any IKE policies.

In order to establish secure communication over the Internet with the remote site you need to configure matching VPN policies on both the local and remote FVS318v3 VPN Firewalls. The outbound VPN policy on one end must match to the inbound VPN policy on other end, and vice versa.

When the network traffic enters into the FVS318v3 from the LAN network interface, if there is no VPN policy found for a type of network traffic, then that traffic passes through without any change. However, if the traffic is selected by a VPN policy, then the IPSec authentication and encryption rules are applied to it as defined in the VPN policy.

By default, a new VPN policy is added with the least priority, that is, at the end of the VPN policy table.

Using Automatic Key Management

The most common configuration scenarios will use IKE policies to automatically manage the authentication and encryption keys. Based on the IKE policy, some parameters for the VPN tunnel are generated automatically. The IKE protocols perform negotiations between the two VPN endpoints to automatically generate required parameters.

Some organizations will use an IKE policy with a Certificate Authority (CA) to perform authentication. Typically, CA authentication is used in large organizations that maintain their own internal CA server. This requires that each VPN gateway have a certificate from the CA. Using CAs reduces the amount of data entry required on each VPN endpoint.

IKE Policies' Automatic Key and Authentication Management

Click the **IKE Policies** link from the VPN section of the main menu, and then click the **Add** button of the IKE Policies screen to display the IKE Policy Configuration menu shown in Figure 6-2.

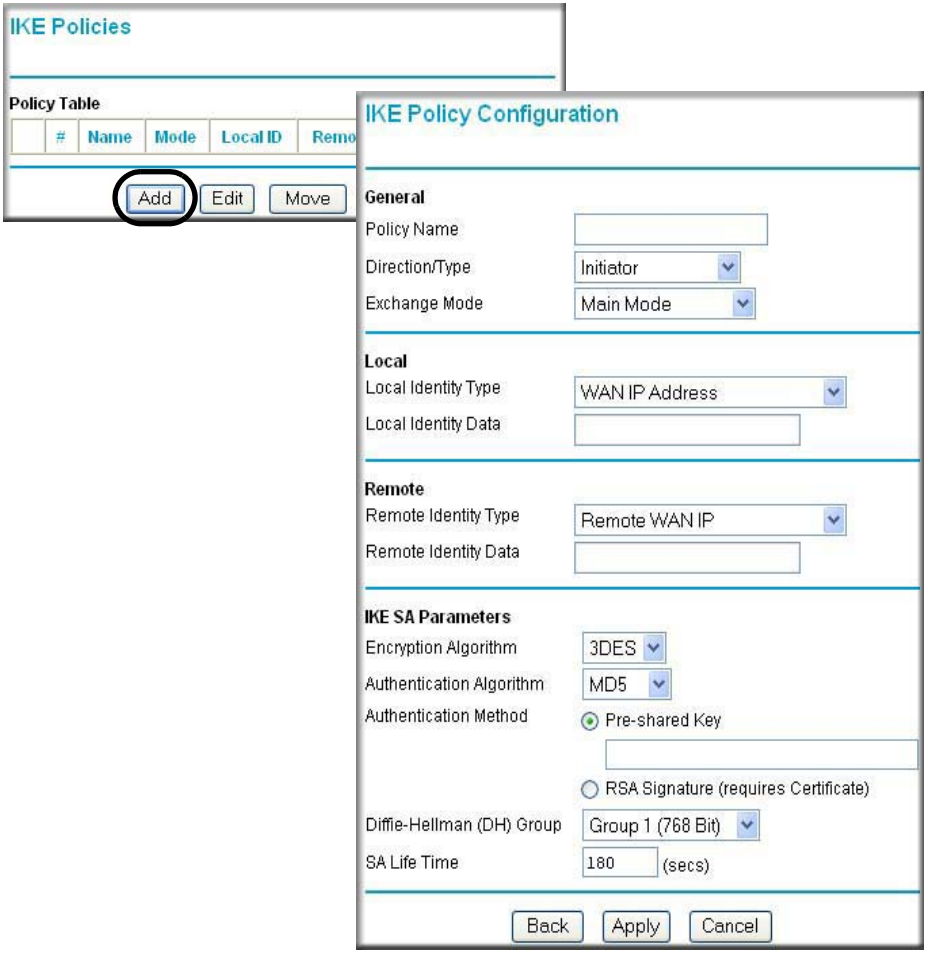


Figure 6-2: IKE - Policy Configuration Menu

The IKE Policy Configuration fields are defined in the following table.

Table 6-1. IKE Policy Configuration fields

Field	Description
General	These settings identify this policy and determine its major characteristics.
Policy Name	The descriptive name of the IKE policy. Each policy should have a unique policy name. This name is not supplied to the remote VPN endpoint. It is only used to help you identify IKE policies.
Direction/Type	This setting is used when determining if the IKE policy matches the current traffic. The drop-down menu includes the following: • Initiator — Outgoing connections are allowed, but incoming are blocked. • Responder — Incoming connections are allowed, but outgoing are blocked. • Both Directions — Both outgoing and incoming connections are allowed. • Remote Access — This is to allow only incoming client connections, where the IP address of the remote client is unknown. If Remote Access is selected, the Exchange Mode must be Aggressive, and the Identities below (both Local and Remote) must be Name. On the matching VPN Policy, the IP address of the remote VPN endpoint should be set to 0.0.0.0.
Exchange Mode	Main Mode or Aggressive Mode. This setting must match the setting used on the remote VPN endpoint. • Main Mode is slower but more secure. Also, the Identity below must be established by IP address. • Aggressive Mode is faster but less secure. The Identity below can be by name (host name, domain name, and e-mail address) instead of by IP address.
Local	These parameters apply to the Local FVS318v3 VPN Firewall.
Local Identity Type	Use this field to identify the local FVS318v3. You can choose one of the following four options from the drop-down list: • By its Internet (WAN) port IP address. • By its Fully Qualified Domain Name (FQDN) — your domain name. • By a Fully Qualified User Name — your name, E-mail address, or other ID. • By DER ASN.1 DN — the binary DER encoding of your ASN.1 X.500 Distinguished Name.
Local Identity Data	This field lets you identify the local FVS318v3 by name.

Table 6-1. IKE Policy Configuration fields

Field	Description
Remote	These parameters apply to the target remote FVS318v3, VPN gateway, or VPN client.
Remote Identity Type	Use this field to identify the remote FVS318v3. You can choose one of the following four options from the drop-down list: • By its Internet (WAN) port IP address. • By its Fully Qualified Domain Name (FQDN) — your domain name. • By a Fully Qualified User Name — your name, E-mail address, or other ID. • By DER ASN.1 DN — the binary DER encoding of your ASN.1 X.500 Distinguished Name.
Remote Identity Data	This field lets you identify the target remote FVS318v3 by name.
IKE SA Parameters	These parameters determine the properties of the IKE Security Association.
Encryption Algorithm	Choose the encryption algorithm for this IKE policy: • DES is the default • 3DES is more secure
Authentication Algorithm	If you enable Authentication Header (AH), this menu lets you to select from these authentication algorithms: • MD5 — the default • SHA-1 — more secure
Authentication Method	You may select Pre-Shared Key or RSA Signature.
Pre-Shared Key	Specify the key according to the requirements of the Authentication Algorithm you selected. • For MD5, the key length should be 16 bytes. • For SHA-1, the key length should be 20 bytes.
RSA Signature	RSA Signature requires a certificate.
Diffie-Hellman (D-H) Group	The DH Group setting determines the bit size used in the key exchange. This must match the value used on the remote VPN gateway or client.
SA Life Time	The amount of time in seconds before the Security Association expires; over an hour (3600) is common.

VPN Policy Configuration for Auto Key Negotiation

An already defined IKE policy is required for VPN - Auto Policy configuration. From the VPN Policies section of the main menu, you can navigate to the VPN - Auto Policy configuration menu.

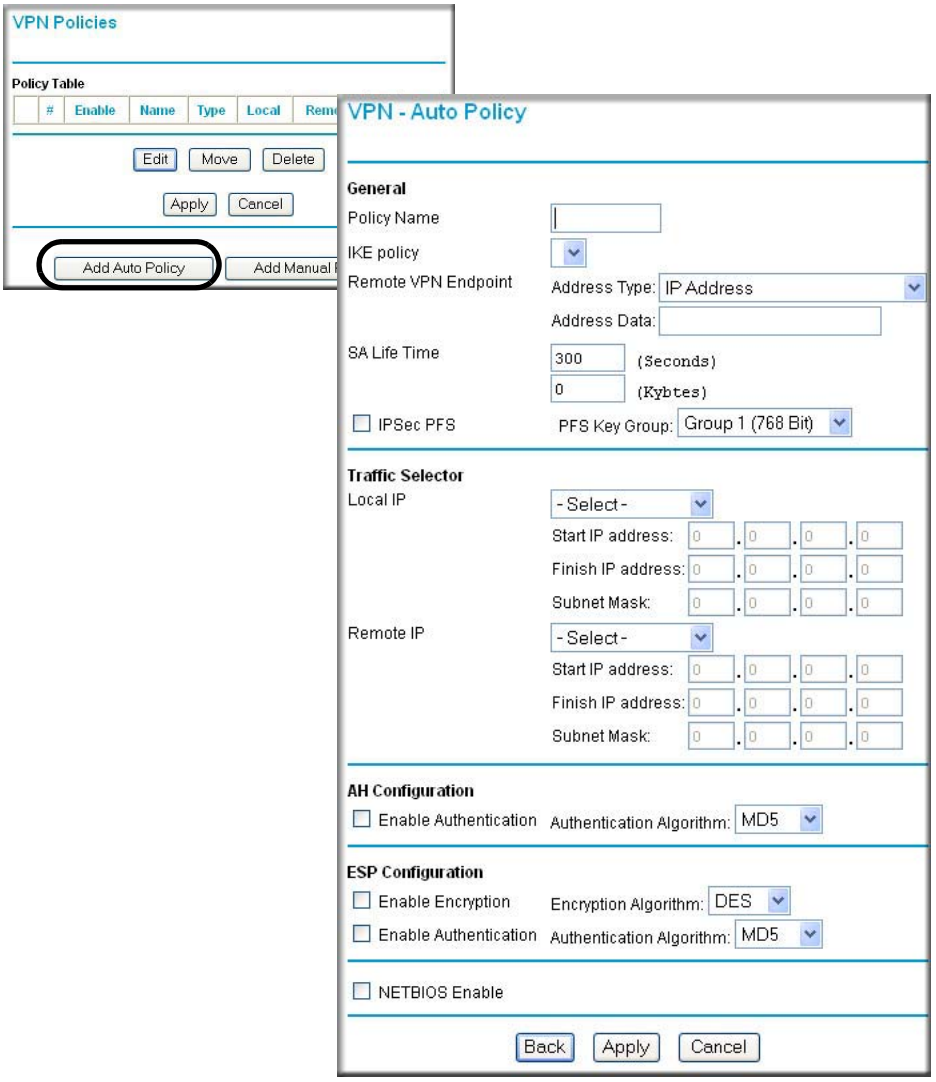


Figure 6-3: VPN - Auto Policy menu

The VPN – Auto Policy fields are defined in the following table.

Table 6-1. VPN – Auto Policy Configuration Fields

Field	Description
General	These settings identify this policy and determine its major characteristics.
Policy Name	The descriptive name of the VPN policy. Each policy should have a unique policy name. This name is not supplied to the remote VPN endpoint. It is only used to help you identify VPN policies.
IKE Policy	The existing IKE policies are presented in a drop-down list. **Note:** Create the IKE policy BEFORE creating a VPN - Auto policy.
Remote VPN Endpoint	The address used to locate the remote VPN firewall or client to which you wish to connect. The remote VPN endpoint must have this FVS318v3's Local IP values entered as its Remote VPN Endpoint. • By its Fully Qualified Domain Name (FQDN) — your domain name. • By its IP Address.
Address Type	The address type used to locate the remote VPN firewall or client to which you wish to connect. • By its Fully Qualified Domain Name (FQDN) — your domain name. • By its IP Address.
Address Data	The address used to locate the remote VPN firewall or client to which you wish to connect. The remote VPN endpoint must have this FVS318v3's Local Identity Data entered as its Remote VPN Endpoint. • By its Fully Qualified Domain Name (FQDN) — your domain name. • By its IP Address.
SA Life Time	The duration of the Security Association before it expires. • Seconds — the amount of time before the SA expires. Over an hour is common (3600). • Kbytes — the amount of traffic before the SA expires. One of these can be set without setting the other.
IPSec PFS	If enabled, security is enhanced by ensuring that the key is changed at regular intervals. Also, even if one key is broken, subsequent keys are no easier to break. Each key has no relationship to the previous key.
PFS Key Group	If PFS is enabled, this setting determines the DH group bit size used in the key exchange. This must match the value used on the remote gateway.

Table 6-1. VPN – Auto Policy Configuration Fields

Field	Description
Traffic Selector	These settings determine if and when a VPN tunnel will be established. If network traffic meets *all* criteria, then a VPN tunnel will be created.
Local IP	The drop-down menu allows you to configure the source IP address of the outbound network traffic for which this VPN policy will provide security. Usually, this address is from your network address space. The choices are: • ANY for all valid IP addresses in the Internet address space • Single IP Address • Range of IP Addresses • Subnet Address
Remote IP	The drop-down menu allows you to configure the destination IP address of the outbound network traffic for which this VPN policy will provide security. Usually, this address is from the remote site's corporate network address space. The choices are: • ANY for all valid IP addresses in the Internet address space • Single IP Address • Range of IP Addresses • Subnet Address
Authenticating Header (AH) Configuration	AH specifies the authentication protocol for the VPN header. These settings must match the remote VPN endpoint.
Enable Authentication	Use this check box to enable or disable AH for this VPN policy.
Authentication Algorithm	If you enable AH, then select the authentication algorithm: • MD5 — the default • SHA1 — more secure
Encapsulated Security Payload (ESP) Configuration	ESP provides security for the payload (data) sent through the VPN tunnel. Generally, you will want to enable both Encryption and Authentication. Two ESP modes are available: • Plain ESP encryption • ESP encryption with authentication These settings must match the remote VPN endpoint.
Enable Encryption	Use this check box to enable or disable ESP Encryption.
Encryption Algorithm	If you enable ESP encryption, then select the encryption algorithm: • DES — the default • 3DES — more secure
Enable Authentication	Use this check box to enable or disable ESP transform for this VPN policy. You can select the ESP mode also with this menu. Two ESP modes are available: • Plain ESP • ESP with authentication

Table 6-1. VPN – Auto Policy Configuration Fields

Field	Description
Authentication Algorithm	If you enable AH, then use this menu to select which authentication algorithm will be employed. The choices are: • MD5 — the default • SHA1 — more secure
NETBIOS Enable	Check this if you wish NETBIOS traffic to be forwarded over the VPN tunnel. The NETBIOS protocol is used by Microsoft Networking for such features as Network Neighborhood.

VPN Policy Configuration for Manual Key Exchange

With Manual Key Management, you will not use an IKE policy. You must manually type in all the required key information. Click the **VPN Policies** link from the VPN section of the main menu to display the menu shown below.

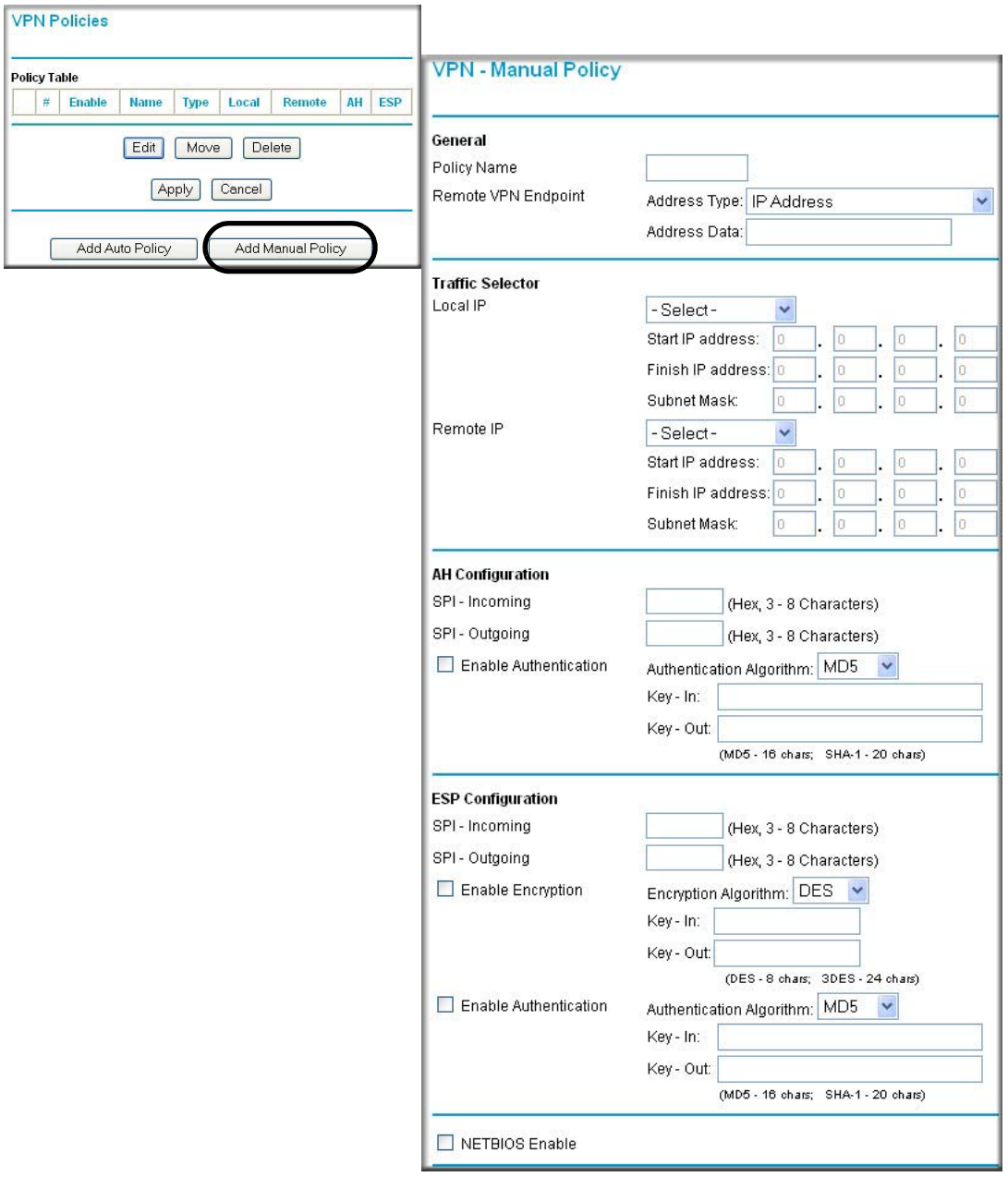


Figure 6-4: VPN - Manual Policy menu

The VPN Manual Policy fields are defined in the following table.

Table 6-1. VPN Manual Policy Configuration Fields

Field	Description
General	These settings identify this policy and determine its major characteristics.
Policy Name	The name of the VPN policy. Each policy should have a unique policy name. This name is not supplied to the remote VPN Endpoint. It is used to help you identify VPN policies.
Remote VPN Endpoint	The WAN Internet IP address of the remote VPN firewall or client to which you wish to connect. The remote VPN endpoint must have this FVS318v3's WAN Internet IP address entered as its Remote VPN Endpoint.
Traffic Selector	These settings determine if and when a VPN tunnel will be established. If network traffic meets *all* criteria, then a VPN tunnel will be created.
Local IP	The drop down menu allows you to configure the source IP address of the outbound network traffic for which this VPN policy will provide security. Usually, this address is from your network address space. The choices are: • ANY for all valid IP addresses in the Internet address space • Single IP Address • Range of IP Addresses • Subnet Address
Remote IP	The drop down menu allows you to configure the destination IP address of the outbound network traffic for which this VPN policy will provide security. Usually, this address is from the remote site's corporate network address space. The choices are: • ANY for all valid IP addresses in the Internet address space • Single IP Address • Range of IP Addresses • Subnet Address
Authenticating Header (AH) Configuration	AH specifies the authentication protocol for the VPN header. These settings must match the remote VPN endpoint. **Note:** The Incoming settings here must match the Outgoing settings on the remote VPN endpoint, and the Outgoing settings here must match the Incoming settings on the remote VPN endpoint.
SPI - Incoming	Enter a hexadecimal value (3 - 8 chars). Any value is acceptable, provided the remote VPN endpoint has the same value in its Outgoing SPI field.
SPI - Outgoing	Enter a hexadecimal value (3 - 8 chars). Any value is acceptable, provided the remote VPN endpoint has the same value in its Incoming SPI field.
Enable Authentication	Use this check box to enable or disable AH. Authentication is often not used. In this case, leave the check box unchecked.

Table 6-1. VPN Manual Policy Configuration Fields

Field	Description
Authentication Algorithm	If you enable AH, then select the authentication algorithm: • MD5 — the default • SHA1 — more secure Enter the keys in the fields provided. For MD5, the keys should be 16 characters. For SHA-1, the keys should be 20 characters.
Key - In	Enter the keys. • For MD5, the keys should be 16 characters. • For SHA-1, the keys should be 20 characters. Any value is acceptable, provided the remote VPN endpoint has the same value in its Authentication Algorithm Key - Out field.
Key - Out	Enter the keys in the fields provided. • For MD5, the keys should be 16 characters. • For SHA-1, the keys should be 20 characters. Any value is acceptable, provided the remote VPN endpoint has the same value in its Authentication Algorithm Key - In field.
Encapsulated Security Payload (ESP) Configuration	ESP provides security for the payload (data) sent through the VPN tunnel. Generally, you will want to enable both encryption and authentication. when you use ESP. Two ESP modes are available: • Plain ESP encryption • ESP encryption with authentication These settings must match the remote VPN endpoint.
SPI - Incoming	Enter a hexadecimal value (3 - 8 chars). Any value is acceptable, provided the remote VPN endpoint has the same value in its Outgoing SPI field.
SPI - Outgoing	Enter a hexadecimal value (3 - 8 chars). Any value is acceptable, provided the remote VPN endpoint has the same value in its Incoming SPI field.
Enable Encryption	Use this check box to enable or disable ESP Encryption.
Encryption Algorithm	If you enable ESP Encryption, then select the Encryption Algorithm: • DES — the default • 3DES — more secure
Key - In	Enter the key in the fields provided. • For DES, the key should be eight characters. • For 3DES, the key should be 24 characters. Any value is acceptable, provided the remote VPN endpoint has the same value in its Encryption Algorithm Key - Out field.
Key - Out	Enter the key in the fields provided. • For DES, the key should be eight characters. • For 3DES, the key should be 24 characters. Any value is acceptable, provided the remote VPN endpoint has the same value in its Encryption Algorithm Key - In field.

Table 6-1. VPN Manual Policy Configuration Fields

Field	Description
Enable Authentication	Use this check box to enable or disable ESP authentication for this VPN policy.
Authentication Algorithm	If you enable authentication, then use this menu to select the algorithm: • MD5 — the default • SHA1 — more secure
Key - In	Enter the key. • For MD5, the key should be 16 characters. • For SHA-1, the key should be 20 characters. Any value is acceptable, provided the remote VPN endpoint has the same value in its Authentication Algorithm Key - Out field.
Key - Out	Enter the key in the fields provided. • For MD5, the key should be 16 characters. • For SHA-1, the key should be 20 characters. Any value is acceptable, provided the remote VPN endpoint has the same value in its Authentication Algorithm Key - In field.
NETBIOS Enable	Check this if you wish NETBIOS traffic to be forwarded over the VPN tunnel. The NETBIOS protocol is used by Microsoft Networking for such features as Network Neighborhood.

Using Digital Certificates for IKE Auto-Policy Authentication

Digital certificates are strings generated using encryption and authentication schemes that cannot be duplicated by anyone without access to the different values used in the production of the string. They are issued by Certification Authorities (CAs) to authenticate a person or a workstation uniquely. The CAs are authorized to issue these certificates by Policy Certification Authorities (PCAs), who are in turn certified by the Internet Policy Registration Authority (IPRA). The FVS318v3 is able to use certificates to authenticate users at the end points during the IKE key exchange process.

The certificates can be obtained from a certificate server that an organization might maintain internally or from the established public CAs. The certificates are produced by providing the particulars of the user being identified to the CA. The information provided may include the user's name, e-mail ID, and domain name.

Each CA has its own certificate. The certificates of a CA are added to the FVS318v3 and then can be used to form IKE policies for the user. Once a CA certificate is added to the FVS318v3 and a certificate is created for a user, the corresponding IKE policy is added to the FVS318v3. Whenever the user tries to send traffic through the FVS318v3, the certificates are used in place of pre-shared keys during initial key exchange as the authentication and key generation mechanism. Once the keys are established and the tunnel is set up the connection proceeds according to the VPN policy.

Certificate Revocation List (CRL)

Each Certification Authority (CA) maintains a list of the revoked certificates. The list of these revoked certificates is known as the Certificate Revocation List (CRL).

Whenever an IKE policy receives the certificate from a peer, it checks for this certificate in the CRL on the FVS318v3 obtained from the corresponding CA. If the certificate is not present in the CRL it means that the certificate is not revoked. IKE can then use this certificate for authentication. If the certificate is present in the CRL it means that the certificate is revoked, and the IKE will not authenticate the client.

You must manually update the FVS318v3 CRL regularly in order for the CA-based authentication process to remain valid.

Walk-Through of Configuration Scenarios on the FVS318v3

There are a variety of configurations you might implement with the FVS318v3. The scenarios listed below illustrate typical configurations you might use in your organization.

In order to help make it easier to set up an IPsec system, the following two scenarios are provided. These scenarios were developed by the VPN Consortium (*http://www.vpnc.org*). The goal is to make it easier to get the systems from different vendors to interoperate. NETGEAR is providing you with both of these scenarios in the following two formats:

- VPN Consortium Scenarios without any product implementation details
- VPN Consortium Scenarios based on the FVS318v3 User Interface

The purpose of providing these two versions of the same scenarios is to help you determine where the two vendors use different vocabulary. Seeing the examples presented in these different ways will reveal how systems from different vendors do the same thing.

The PC must have the NETGEAR ProSafe VPN Client program installed that supports IPSec. Go to the NETGEAR Web site (*http://www.netgear.com*) and select VPN01L_VPN05L in the Product Quick Find drop down menu for information on how to purchase the NETGEAR ProSafe VPN Client.

	Note: Before installing the NETGEAR ProSafe VPN Client software, be sure to turn off any virus protection or firewall software you may be running on your PC.

VPN Consortium Scenario 1: Gateway-to-Gateway with Preshared Secrets

The following is a typical gateway-to-gateway VPN that uses a preshared secret for authentication.

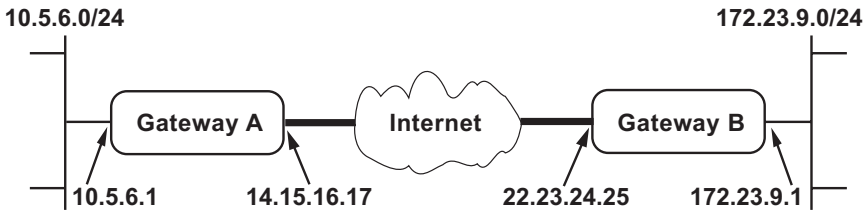


Figure 6-5: VPN Consortium Scenario 1

Gateway A connects the internal LAN 10.5.6.0/24 to the Internet. Gateway A's LAN interface has the address 10.5.6.1, and its WAN (Internet) interface has the address 14.15.16.17.

Gateway B connects the internal LAN 172.23.9.0/24 to the Internet. Gateway B's WAN (Internet) interface has the address 22.23.24.25. Gateway B's LAN interface address, 172.23.9.1, can be used for testing IPsec but is not needed for configuring Gateway A.

The IKE Phase 1 parameters used in Scenario 1 are:

- Main mode
- TripleDES
- SHA-1
- MODP group 2 (1024 bits)
- pre-shared secret of “hr5xb84l6aa9r6”
- SA lifetime of 28800 seconds (eight hours) with no kilobytes rekeying

The IKE Phase 2 parameters used in Scenario 1 are:

- TripleDES
- SHA-1
- ESP tunnel mode
- MODP group 2 (1024 bits)
- Perfect forward secrecy for rekeying
- SA lifetime of 3600 seconds (one hour) with no kilobytes rekeying
- Selectors for all IP protocols, all ports, between 10.5.6.0/24 and 172.23.9.0/24, using IPv4 subnets

FVS318v3 Scenario 1: FVS318v3 to Gateway B IKE and VPN Policies

Note: This scenario assumes all ports are open on the FVS318v3. You can verify this by reviewing the security settings as seen in the Figure 4-2 on page 4-3.

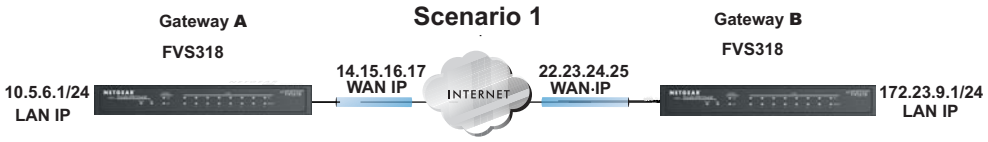


Figure 6-6: LAN to LAN VPN access from an FVS318v3 to an FVS318v3

Use this scenario illustration and configuration screens as a model to build your configuration.

1. **Log in to the FVS318v3 labeled Gateway A as in the illustration.**

   Log in at the default address of *http://192.168.0.1* with the default user name of **admin** and default password of **password**, or using whatever password and LAN address you have chosen.

2. **Configure the WAN (Internet) and LAN IP addresses of the FVS318v3.**

   a. From the main menu Setup section, click the **Basic Setup** link to go back to the Basic Settings menu.

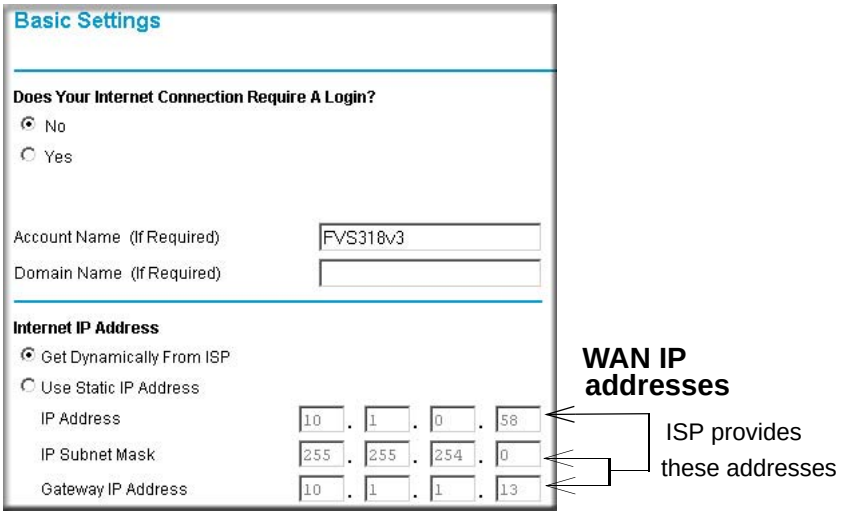


Figure 6-7: FVS318v3 Internet IP Address menu

b. Configure the WAN Internet Address according to the settings above and click **Apply** to save your settings. For more information on configuring the WAN IP settings in the Basic Settings topics, please see "How to Manually Configure Your Internet Connection" on page 3-12.

c. From the main menu Advanced section, click the **LAN IP Setup** link. The following menu appears

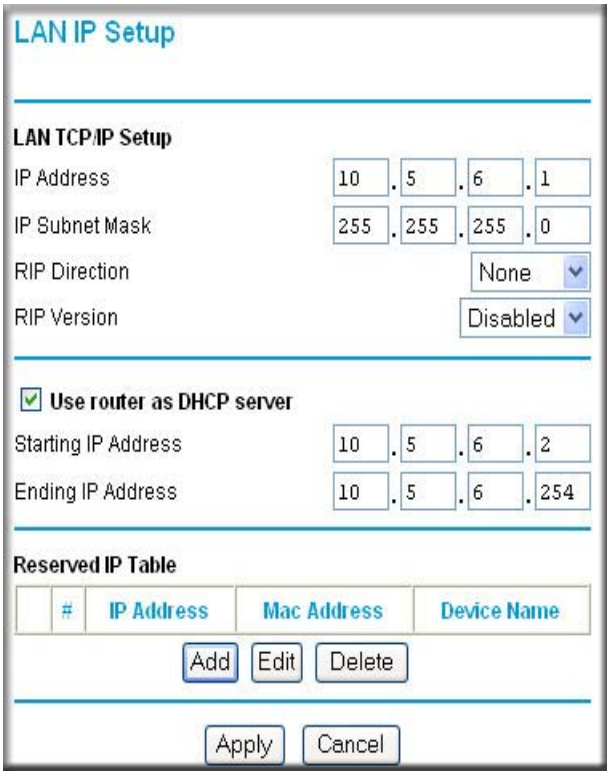


Figure 6-8: LAN IP Setup menu

d. Configure the LAN IP address according to the settings above and click **Apply** to save your settings. For more information on LAN TCP/IP setup topics, please see "Configuring LAN TCP/IP Setup Parameters" on page 8-3.

Note: After you click **Apply** to change the LAN IP address settings, your workstation will be disconnected from the FVS318v3. You will have to log on with *http://10.5.6.1* which is now the address you use to connect to the built-in Web-based configuration manager of the FVS318v3.

3. Set up the IKE Policy illustrated below on the FVS318v3.

a. From the main menu VPN section, click on the **IKE Policies** link, and then click the **Add** button to display the screen below.

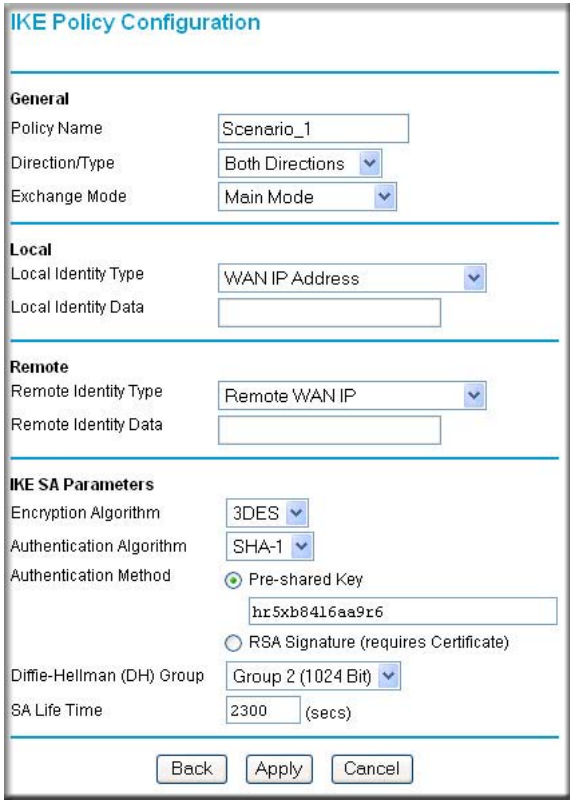


Figure 6-9: Scenario 1 IKE Policy

b. Configure the IKE Policy according to the settings in the illustration above and click **Apply** to save your settings. For more information on IKE Policy topics, please see "IKE Policies' Automatic Key and Authentication Management" on page 6-3.

4. Set up the FVS318v3 VPN -Auto Policy illustrated below.

a. From the main menu VPN section, click on the **VPN Policies** link, and then click on the **Add Auto Policy** button.

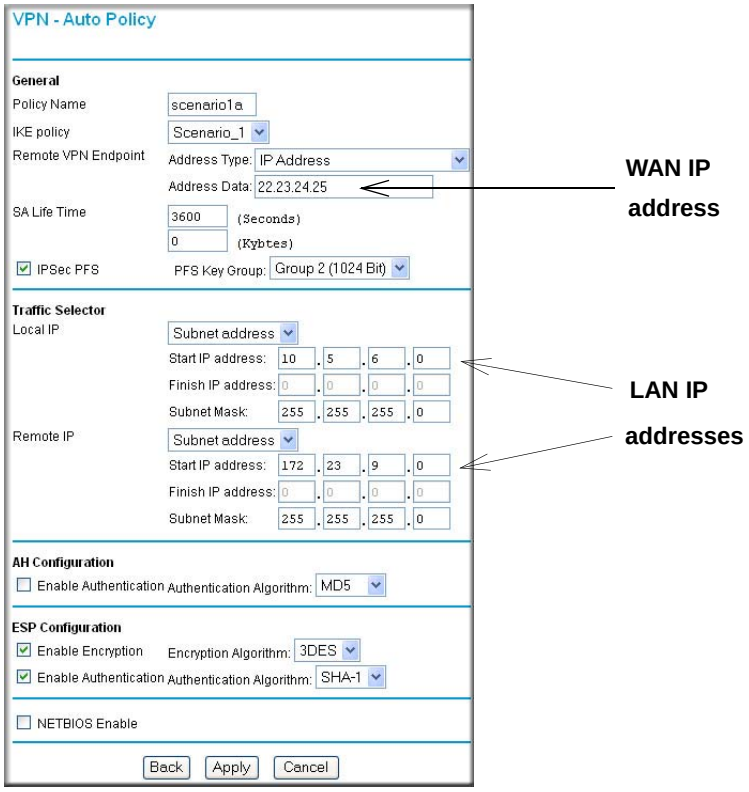


Figure 6-10: Scenario 1 VPN - Auto Policy

b. Configure the IKE Policy according to the settings in the illustration above and click **Apply** to save your settings. For more information on IKE Policy topics, please see "IKE Policies' Automatic Key and Authentication Management" on page 6-3.

5. **After applying these changes, all traffic from the range of LAN IP addresses specified on FVS318v3 A and FVS318v3 B will flow over a secure VPN tunnel.**

How to Check VPN Connections

You can test connectivity and view VPN status information on the FVS318v3 (see also "VPN Tunnel Control" on page 5-26).

Testing the Gateway A FVS318v3 LAN and the Gateway B LAN

1. Using our example, from a PC attached to the FVS318v3 on LAN A, on a Windows PC click the **Start** button on the taskbar and then click **Run**.
2. Type **ping -t 172.23.9.1**, and then click **OK**.
3. This will cause a continuous ping to be sent to the LAN interface of Gateway B. Within two minutes, the ping response should change from timed out to reply.
4. At this point the connection is established.
5. To test connectivity between the FVS318v3 Gateway A and Gateway B WAN ports, follow these steps:
   a. Using our example, log in to the FVS318v3 on LAN A, go to the main menu Maintenance section and click the **Diagnostics** link.
   b. To test connectivity to the WAN port of Gateway B, enter **22.23.24.25**, and then click **Ping**.
   c. This causes a ping to be sent to the WAN interface of Gateway B. Within two minutes, the ping response should change from timed out to reply. You may have to run this test several times before you get the reply message back from the target FVS318v3.
   d. At this point the connection is established.

   Note: If you want to ping the FVS318v3 as a test of network connectivity, be sure the FVS318v3 is configured to respond to a ping on the Internet WAN port by checking the check box seen in Figure 4-2 on page 4-3. However, to preserve a high degree of security, you should turn off this feature when you are finished with testing.
6. To view the FVS318v3 event log and status of Security Associations, follow these steps:
   a. Go to the FVS318v3 main menu VPN section and click the **VPN Status** link.
   b. The log screen displays a history of the VPN connections, and the IPSec SA and IKE SA tables will report the status and data transmission statistics of the VPN tunnels for each policy.

FVS318v3 Scenario 2: FVS318v3 to FVS318v3 with RSA Certificates

The following is a typical gateway-to-gateway VPN that uses Public Key Infrastructure x.509 (PKIX) certificates for authentication. The network setup is identical to the one given in Scenario 1. The IKE Phase 1 and Phase 2 parameters are identical to the ones given in Scenario 1, with the exception that the identification is done with signatures authenticated by PKIX certificates.

Note: Before completing this configuration scenario, make sure the correct Time Zone is set on the FVS318v3. For instructions on this topic, see "Time Zone" on page 4-13.

1. **Obtain a root certificate.**
   a. Obtain the root certificate (that includes the public key) from a Certificate Authority (CA)

      Note: The procedure for obtaining certificates differs from a CA like Verisign and a CA such as a Windows 2000 certificate server, which an organization operates for providing certificates for its members. For example, an administrator of a Windows 2000 certificate server might provide it to you via e-mail.

   b. Save the certificate as a text file called *trust.txt*.
2. **Install the trusted CA certificate for the Trusted Root CA.**
   a. Log in to the FVS318v3.
   b. From the main menu VPN section, click the **CAs** link.
   c. Click **Add** to add a CA.
   d. Click **Browse** to locate the *trust.txt* file.
   e. Click **Upload**.
3. **Create a certificate request for the FVS318v3.**
   a. From the main menu VPN section, click the **Certificates** link.

b. Click the **Generate Request** button to display the screen illustrated in Figure 6-11 below.

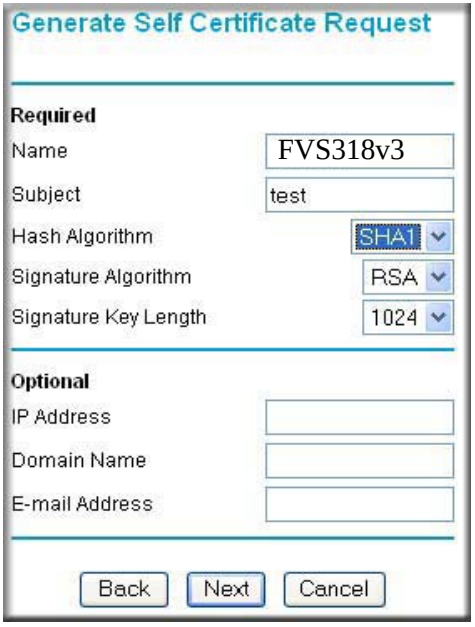


Figure 6-11: Generate Self Certificate Request menu

c. Fill in the fields on the Add Self Certificate screen.

- Required
  - Name. Enter a name to identify this certificate.
  - Subject. This is the name that other organizations will see as the holder (owner) of this certificate. This should be your registered business name or official company name. Generally, all certificates should have the same value in the Subject field.
  - Hash Algorithm. Select the desired option: MD5 or SHA1.
  - Signature Algorithm. Select the desired option: DSS or RSA.
  - Signature Key Length. Select the desired option: 512, 1024, or 2048.
- Optional
  - IP Address. If you use “IP type” in the IKE policy, you should input the IP Address here. Otherwise, you should leave this blank.

– Domain Name. If you have a domain name, you can enter it here. Otherwise, you should leave this blank.

– E-mail Address. You can enter you e-mail address here.

d. Click the **Next** button to continue. The FVS318v3 generates a Self Certificate Request as shown below.

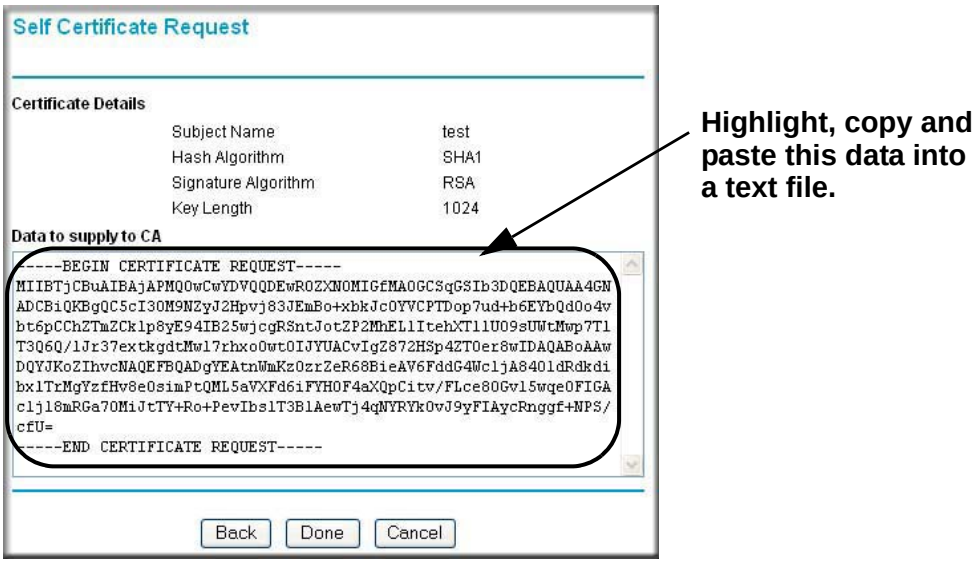


Figure 6-12: Self Certificate Request data

4. Transmit the Self Certificate Request data to the Trusted Root CA.

a. Highlight the text in the Data to supply to CA area, copy it, and paste it into a text file.

b. Give the certificate request data to the CA. In the case of a Windows 2000 internal CA, you might simply e-mail it to the CA administrator. The procedures of a CA like Verisign and a CA such as a Windows 2000 certificate server administrator will differ. Follow the procedures of your CA.

c. When you have finished gathering the Self Certificate Request data, click the **Done** button. You will return to the Certificates screen where your pending "FVS318v3" Self Certificate Request will be listed, as illustrated in Figure 6-13 below.

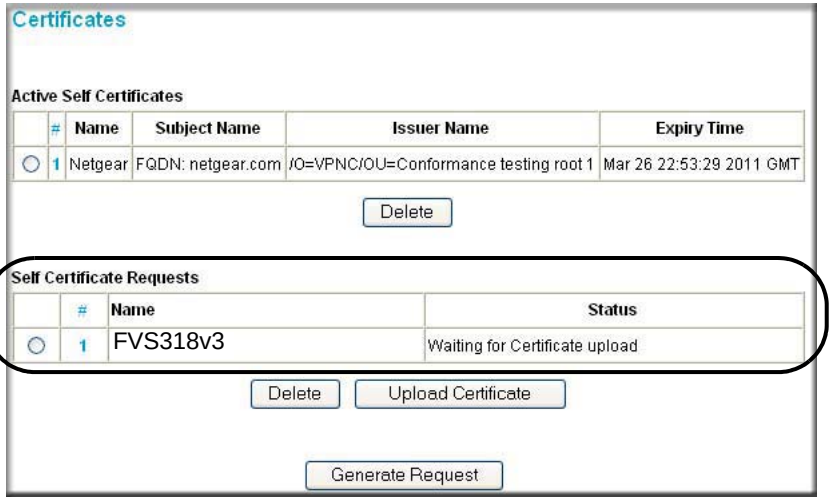


Figure 6-13: Self Certificate Requests table

5. Receive the certificate back from the Trusted Root CA and save it as a text file.

Note: In the case of a Windows 2000 internal CA, the CA administrator might simply email it to back to you. Follow the procedures of your CA. Save the certificate you get back from the CA as a text file called *final.txt*.

6. Upload the new certificate.

a. From the main menu VPN section, click the **Certificates** link.

b. Click the radio button of the Self Certificate Request you want to upload.

c. Click the **Upload Certificate** button.

d. Browse to the location of the file you saved in Step 5 above that contains the certificate from the CA.

e. Click the **Upload** button.

f. You will now see the “FVS318v3” entry in the Active Self Certificates table and the pending “FVS318v3” Self Certificate Request is gone, as illustrated below.

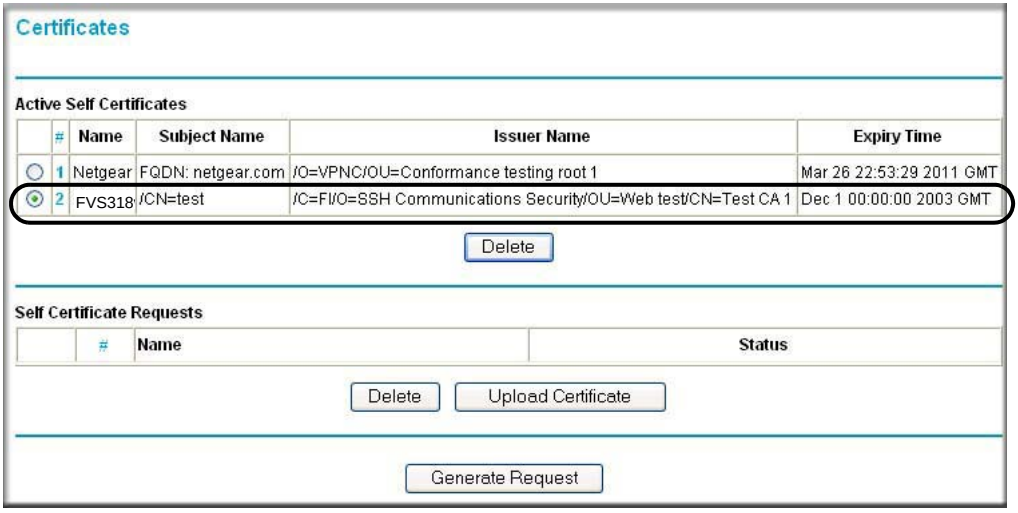

Certificates
Active Self Certificates
Name Subject Name Issuer Name Expiry Time
1 Netgear FQDN: netgear.com /O=VPNC/OU=Conformance testing root 1 Mar 26 22:53:29 2011 GMT
2 FVS318 /CN=test /C=FI/O=SSH Communications Security/OU=Web test/CN=Test CA 1 Dec 1 00:00:00 2003 GMT
Delete
Self Certificate Requests
Name Status
Delete
Upload Certificate
Generate Request

Figure 6-14: Self Certificates table

7. Associate the new certificate and the Trusted Root CA certificate on the FVS318v3.

a. Create a new IKE policy called **Scenario_2** with all the same properties of **Scenario_1** (see “Scenario 1 IKE Policy” on page 6-19) except now use the RSA Signature instead of the shared key.

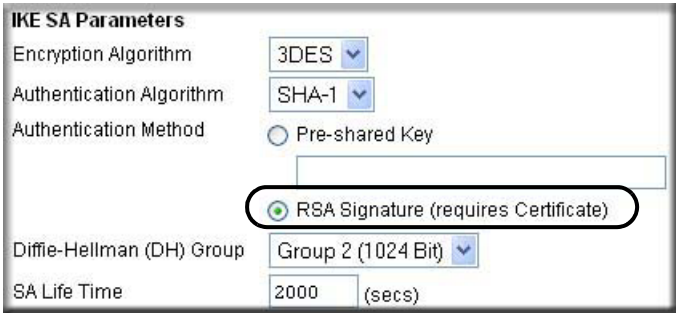


Figure 6-15: IKE policy using RSA Signature

b. Create a new VPN Auto Policy called **scenario2a** with all the same properties as **scenario1a** except that it uses the IKE policy called Scenario_2.

Now, the traffic from devices within the range of the LAN subnet addresses on FVS318v3 A and Gateway B will be authenticated using the certificates rather than via a shared key.

8. Set up Certificate Revocation List (CRL) checking.

a. Get a copy of the CRL from the CA and save it as a text file.

Note: The procedure for obtaining a CRL differs from a CA like Verisign and a CA such as a Windows 2000 certificate server, which an organization operates for providing certificates for its members. Follow the procedures of your CA.

b. From the main menu VPN section, click the **CRL** link.

c. Click **Add** to add a CRL.

d. Click **Browse** to locate the CRL file.

e. Click **Upload**.

Now expired or revoked certificates will not be allowed to use the VPN tunnels managed by IKE policies which use this CA.

Note: You must update the CRLs regularly in order to maintain the validity of the certificate-based VPN policies.

Chapter 7
Maintenance

This chapter describes how to use the maintenance features of your FVS318v3 ProSafe VPN Firewall. These features can be found by clicking on the Maintenance heading in the main menu of the browser interface.

Viewing VPN Firewall Status Information

The Router Status menu provides status and usage information. From the main menu of the browser interface, click **Maintenance**, then select **Router Status** to view this screen.

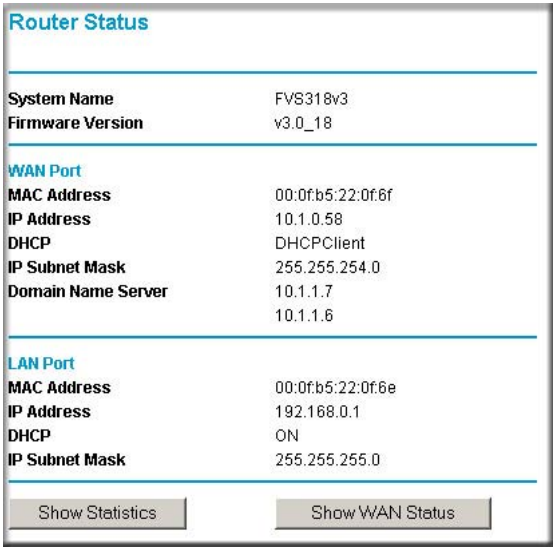


Figure 7-1: Router Status screen

This screen shows the following parameters:

Table 7-1. FVS318v3 Status fields

Field	Description
System Name	The System Name assigned to the firewall.
Firmware Version	The firewall firmware version.
WAN Port	These parameters apply to the Internet (WAN) port of the firewall.
MAC Address	The MAC address used by the Internet (WAN) port of the firewall.
IP Address	The IP address used by the Internet (WAN) port of the firewall. If no address is shown, the firewall cannot connect to the Internet.
IP Subnet Mask	The IP Subnet Mask being used by the Internet (WAN) port of the firewall.
DHCP	The protocol on the WAN port used to obtain the WAN IP address. This field can show DHCP Client, Fixed IP, PPPoE, BPA or PPTP. For example, if set to Client, the firewall is configured to obtain an IP address dynamically from the ISP.
LAN Port	These parameters apply to the Local (WAN) port of the firewall.
MAC Address	The MAC address used by the LAN port of the firewall.
IP Address	The IP address used by the Local (LAN) port of the firewall. The default is 192.168.0.1
IP Subnet Mask	The IP Subnet Mask used by the Local (LAN) port of the firewall. The default is 255.255.255.0
DHCP	Identifies if the firewall's built-in DHCP server is active for the LAN attached devices.

Click **Show WAN Status** to display the WAN connection status.

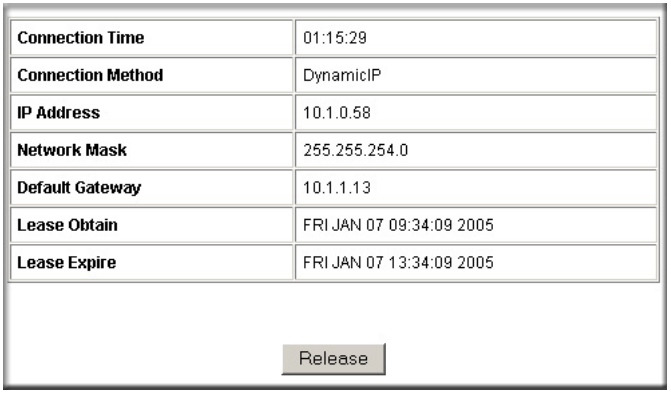


Figure 7-2: WAN Connection Status screen

This screen shows the following statistics:.

Table 7-1. Connection Status fields

Field	Description
Connection Time	The length of time the firewall has been connected to your Internet service provider's network.
Connection Method	The method used to obtain an IP address from your Internet service provider.
IP Address	The WAN (Internet) IP address assigned to the firewall.
Network Mask	The WAN (Internet) subnet mask assigned to the firewall.
Default Gateway	The WAN (Internet) default gateway the firewall communicates with.

Log action buttons are described in Table 7-2

Table 7-2. Connection Status action buttons

Button	Description
Renew	Click the **Renew** button to renew the DHCP lease.

Click **Show Statistics** to display firewall usage statistics.

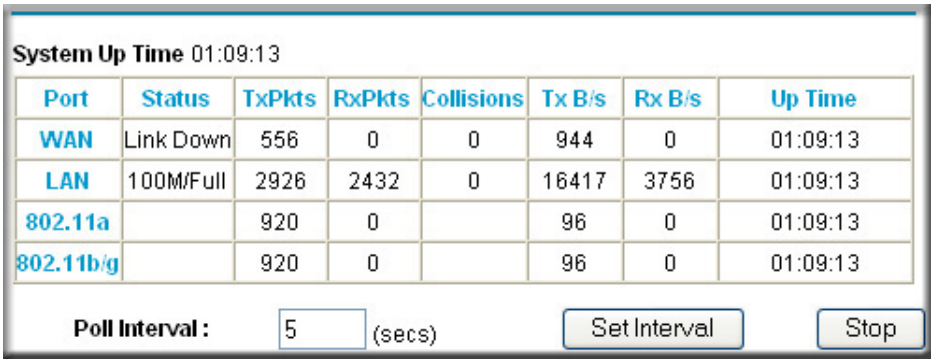


Figure 7-3: Router Statistics screen

This screen shows the following statistics:

Table 7-1. Router Statistics fields

Field	Description
Interface	The statistics for the WAN (Internet), LAN (local), 802.11a, and 802.11b/g interfaces. For each interface, the screen displays:
Status	The link status of the interface.
TxPkts	The number of packets transmitted on this interface since reset or manual clear.
RxPkts	The number of packets received on this interface since reset or manual clear.
Collisions	The number of collisions on this interface since reset or manual clear.
Tx B/s	The current transmission (outbound) bandwidth used on the interfaces.
Rx B/s	The current reception (inbound) bandwidth used on the interfaces.
Up Time	The amount of time since the firewall was last restarted.
Up Time	The time elapsed since this port acquired the link.
Poll Interval	Specifies the intervals at which the statistics are updated in this window. Click on **Stop** to freeze the display.

WAN Status action buttons are described in the table below:

Table 7-2. Connection Status action buttons

Field	Description
Set Interval	Enter a time and click the button to set the polling frequency.
Stop	Click the **Stop** button to freeze the polling information.

Viewing a List of Attached Devices

The Attached Devices menu contains a table of all IP devices that the firewall has discovered on the local network. From the main menu of the browser interface, under the Maintenance heading, select Attached Devices to view the table, shown below.

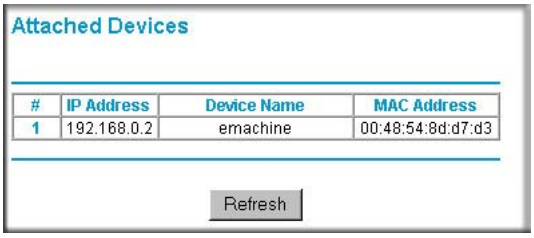


Figure 7-4: Attached Devices menu

For each device, the table shows the IP address, NetBIOS Host Name (if available), and Ethernet MAC address. Note that if the firewall is rebooted, the table data is lost until the firewall rediscovers the devices. To force the firewall to look for attached devices, click the **Refresh** button.

Upgrading the Firewall Software

Note: The FVS318v3 firmware is not backward compatible with earlier versions of the FVS318 firewall.

The routing software of the FVS318v3 VPN Firewall is stored in FLASH memory, and can be upgraded as new software is released by NETGEAR. Upgrade files can be downloaded from NETGEAR's Web site. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN) file before sending it to the firewall. The upgrade file can be sent to the firewall using your browser.

Note: The Web browser used to upload new firmware into the FVS318v3 VPN Firewall must support HTTP uploads. NETGEAR recommends using Microsoft Internet Explorer or Netscape Navigator 5.0 or above.

From the main menu of the browser interface, under the Maintenance heading, select the Router Upgrade heading to display the menu shown below.

Figure 7-5: Router Upgrade menu

To upload new firmware:

1. Download and unzip the new software file from NETGEAR.
2. In the Router Upgrade menu, click the **Browse** button and browse to the location of the binary (.BIN) upgrade file
3. Click **Upload**.

   Note: When uploading software to the FVS318v3 VPN Firewall, it is important not to interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it may corrupt the software. When the upload is complete, your firewall will automatically restart. The upgrade process will typically take about one minute.

In some cases, you may need to reconfigure the firewall after upgrading.

Configuration File Management

The configuration settings of the FVS318v3 VPN Firewall are stored within the firewall in a configuration file. This file can be saved (backed up) to a user's PC, retrieved (restored) from the user's PC, or cleared to factory default settings.

From the main menu of the browser interface, under the Maintenance heading, select the Settings Backup heading to bring up the menu shown below.

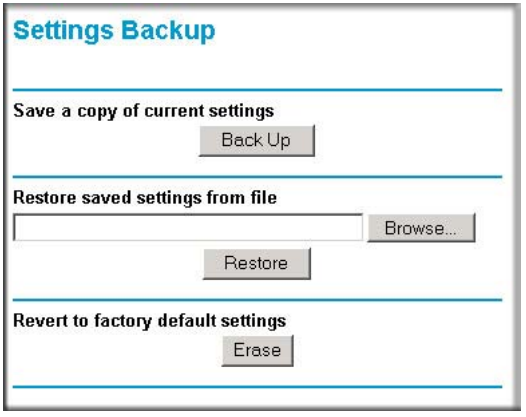


Figure 7-6: Settings Backup menu

You can use the Settings Backup menu to back up your configuration in a file, restore from that file, or erase the configuration settings.

Backing Up the Configuration

To save your settings, select the Backup tab. Click the **Backup** button. Your browser will extract the configuration file from the firewall and prompts you for a location on your PC to store the file. You can give the file a meaningful name at this time, such as sanjose.cfg.

Restoring the Configuration

To restore your settings from a saved configuration file, enter the full path to the file on your PC or click the **Browse** button to browse to the file. When you have located it, click the **Restore** button to send the file to the firewall. The firewall will then reboot automatically.

Erasing the Configuration

It is sometimes desirable to restore the firewall to a known blank condition. To do this, see the Erase function, which will restore all factory settings. After an erase, the firewall's password will be **password**, the LAN IP address will be 192.168.0.1, and the firewall's DHCP client will be enabled.

To erase the configuration, click the **Erase** button.

To restore the factory default configuration settings without knowing the login password or IP address, you must use the reset button on the rear panel of the firewall. See "Restoring the Default Configuration and Password" on page 9-7.

Changing the Administrator Password

The default password for the firewall's Web Configuration Manager is **password**. NETGEAR recommends that you change this password to a more secure password.

From the main menu of the browser interface, under the Maintenance heading, select Set Password to bring up this menu.

Figure 7-7: Set Password menu

To change the password, first enter the old password, and then enter the new password twice. Click **Apply**. To change the login idle timeout, change the number of minutes and click **Apply**.

Chapter 8
Advanced Configuration

This chapter describes how to configure the advanced features of your FVS318v3 ProSafe VPN Firewall. These features can be found under the Advanced heading in the main menu of the browser interface.

How to Configure Dynamic DNS

If your network has a permanently assigned IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned IP address, you will not know in advance what your IP address will be, and the address can change frequently. In this case, you can use a commercial dynamic DNS service, which will allow you to register your domain to their IP address, and will forward traffic directed to your domain to your frequently-changing IP address.

The firewall contains a client that can connect to a dynamic DNS service provider. To use this feature, you must select a service provider and obtain an account with them. After you have configured your account information in the firewall, whenever your ISP-assigned IP address changes, your firewall will automatically contact your dynamic DNS service provider, log in to your account, and register your new IP address.

1. Log in to the firewall at its default LAN address of *http://192.168.0.1* with its default user name of **admin**, default password of **password**, or using whatever password and LAN address you have chosen for the firewall.
2. From the main menu of the browser interface, under Advanced, click on **Dynamic DNS**.
3. Access the Web site of one of the dynamic DNS service providers whose names appear in the menu, and register for an account.
   For example, for dyndns.org, go to *www.dyndns.org*.
4. Select the name of your dynamic DNS Service Provider.
5. Type the host and domain name that your dynamic DNS provider gave you. This will look like a URL, such as *myName.dyndns.org*.
6. Type the user name for your dynamic DNS account.

7. Type the password (or key) for your dynamic DNS account.
8. If your dynamic DNS provider allows the use of wildcards in resolving your URL, you may select the Use wildcards check box to activate this feature.
   For example, the wildcard feature will cause *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org
9. Click **Apply** to save your configuration.

Note: If your ISP assigns a private WAN IP address such as 192.168.x.x or 10.x.x.x, the dynamic DNS service will not work because private addresses will not be routed on the Internet.

Using the LAN IP Setup Options

The LAN IP Setup menu allows configuration of LAN IP services such as DHCP and RIP. From the main menu of the browser interface, under Advanced, click on **LAN IP Setup** to view the menu shown below.

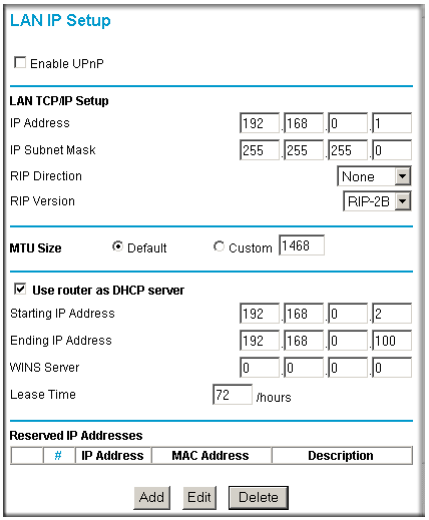


Figure 8-1: LAN IP Setup Menu

Configuring LAN TCP/IP Setup Parameters

The firewall is shipped preconfigured to use private IP addresses on the LAN side, and to act as a DHCP server. The firewall's default LAN IP configuration is:

- LAN IP addresses—192.168.0.1
- Subnet mask—255.255.255.0

These addresses are part of the IETF-designated private address range for use in private networks, and should be suitable in most applications. If your network has a requirement to use a different IP addressing scheme, you can make those changes in this menu.

The LAN IP parameters are:

- IP Address
  This is the LAN IP address of the firewall.
- IP Subnet Mask
  This is the LAN Subnet Mask of the firewall. Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or firewall.
- RIP Direction
  RIP (Router Information Protocol) allows a firewall to exchange routing information with other firewalls. The RIP Direction selection controls how the firewall sends and receives RIP packets. Both is the default.
  - — When set to Both or Out Only, the firewall broadcasts its routing table periodically.
  - — When set to Both or In Only, it incorporates the RIP information that it receives.
  - — When set to None, it will not send any RIP packets and ignores any RIP packets received.
- RIP Version
  This controls the format and the broadcasting method of the RIP packets that the firewall sends. (It recognizes both formats when receiving.) By default, this is set for RIP-1.
  - — RIP-1 is universally supported. RIP-1 is probably adequate for most networks, unless you have an unusual network setup.
  - — RIP-2 carries more information. RIP-2B uses subnet broadcasting.

	Note: If you change the LAN IP address of the firewall while connected through the browser, you will be disconnected. You must then open a new connection to the new IP address and log in again.

Using the Firewall as a DHCP server

By default, the firewall functions as a DHCP (Dynamic Host Configuration Protocol) server, allowing it to assign IP, DNS server, and default gateway addresses to all computers connected to the firewall's LAN. The assigned default gateway address is the LAN address of the firewall. IP addresses will be assigned to the attached PCs from a pool of addresses specified in this menu. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN.

For most applications, the default DHCP and TCP/IP settings of the firewall are satisfactory. See "IP Configuration by DHCP" on page B-10" for an explanation of DHCP and information about how to assign IP addresses for your network.

If another device on your network will be the DHCP server, or if you will manually configure the network settings of all of your computers, clear the **Use router as DHCP server** check box. Otherwise, leave it checked.

To specify the pool of IP addresses to be assigned, set the Starting IP Address and Ending IP Address. These addresses should be part of the same IP address subnet as the firewall's LAN IP address. Using the default addressing scheme, you should define a range between 192.168.0.2 and 192.168.0.253, although you may wish to save part of the range for devices with fixed addresses.

The firewall will deliver the following parameters to any LAN device that requests DHCP:

- An IP address from the range you have defined
- Subnet mask
- Gateway IP address (the firewall's LAN IP address)
- Primary DNS server (if you entered a primary DNS address in the Basic Settings menu; otherwise, the firewall's LAN IP address)
- Secondary DNS server (if you entered a secondary DNS address in the Basic Settings menu

Using Address Reservation

When you specify a reserved IP address for a PC on the LAN, that PC will always receive the same IP address each time it accesses the firewall's DHCP server. Reserved IP addresses should be assigned to servers that require permanent IP settings.

To reserve an IP address:

1. Click the **Add** button.
2. In the IP Address box, type the IP address to assign to the PC or server. (Choose an IP address from the firewall's LAN subnet, such as 192.168.0.X.)
3. Type the MAC Address of the PC or server. (**Tip**: If the PC is already present on your network, you can copy its MAC address from the Attached Devices menu and paste it here.)
4. Click **Apply** to enter the reserved address into the table.

Note: The reserved address will not be assigned until the next time the PC contacts the firewall's DHCP server. Reboot the PC or access its IP configuration and force a DHCP release and renew.

To edit or delete a reserved address entry:

1. Click the button next to the reserved address you want to edit or delete.
2. Click **Edit** or **Delete**.

Configuring Static Routes

Static Routes provide additional routing information to your firewall. Under normal circumstances, the firewall has adequate routing information after it has been configured for Internet access, and you do not need to configure additional static routes. You must configure static routes only for unusual cases such as multiple firewalls or multiple IP subnets located on your network.

From the Main Menu of the browser interface, under Advanced, click on **Static Routes** to view the Static Route table shown below.

Figure 8-2: Static Routes table

To add or edit a Static Route:

1. Click the **Add** button to open the Add/Edit menu, shown below.

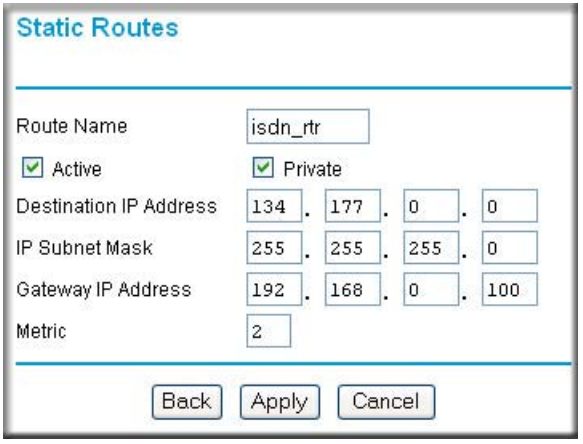


Figure 8-3: Static Route Entry and Edit menu

2. Type a route name for this static route in the Route Name box.
   (This is for identification purpose only.)
3. Select Private if you want to limit access to the LAN only. The static route will not be reported in RIP.
4. Select Active to make this route effective.
5. Type the Destination IP Address of the final destination.
6. Type the IP Subnet Mask for this destination.
   If the destination is a single host, type **255.255.255.255**.
7. Type the Gateway IP Address, which must be a firewall on the same LAN segment as the firewall.

8. Type a number between 1 and 15 as the Metric value.
   This represents the number of firewalls between your network and the destination. Usually, a setting of 2 or 3 works, but if this is a direct connection, set it to 1.
9. Click **Apply** to have the static route entered into the table.

Static Route Example

As an example of when a static route is needed, consider the following case:

- Your primary Internet access is through a cable modem to an ISP.
- You have an ISDN firewall on your home network for connecting to the company where you are employed. This firewall's address on your LAN is 192.168.0.100.
- Your company's network is 134.177.0.0.

When you first configured your firewall, two implicit static routes were created. A default route was created with your ISP as the gateway, and a second static route was created to your local network for all 192.168.0.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your firewall will forward your request to the ISP. The ISP forwards your request to the company where you are employed, and the request will likely be denied by the company's firewall.

In this case you must define a static route, telling your firewall that 134.177.0.0 should be accessed through the ISDN firewall at 192.168.0.100. The static route would look like Figure 8-3.

In this example:

- The Destination IP Address and IP Subnet Mask fields specify that this static route applies to all 134.177.x.x addresses.
- The Gateway IP Address fields specifies that all traffic for these addresses should be forwarded to the ISDN firewall at 192.168.0.100.
- A Metric value of 1 will work since the ISDN firewall is on the LAN.
- Private is selected only as a precautionary security measure in case RIP is activated.

Enabling Remote Management Access

Using the Remote Management page, you can allow a user or users on the Internet to configure, upgrade and check the status of your FVS318v3 VPN Firewall.

	Note: Be sure to change the firewall's default configuration password to a very secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of letters (both upper and lower case), numbers, and symbols. Your password can be up to 30 characters.

To configure your firewall for Remote Management:

1. Select the Turn Remote Management On check box.
2. Specify what external addresses will be allowed to access the firewall's remote management.

   Note: For enhanced security, restrict access to as few external IP addresses as practical.

   a. To allow access from any IP address on the Internet, select Everyone.

   b. To allow access from a range of IP addresses on the Internet, select IP address range. Enter a beginning and ending IP address to define the allowed range.

   c. To allow access from a single IP address on the Internet, select Only this PC. Enter the IP address that will be allowed access.

3. Specify the Port Number that will be used for accessing the management interface.

   Web browser access normally uses the standard HTTP service port 80. For greater security, you can change the remote management web interface to a custom port by entering that number in the box provided. Choose a number between 1024 and 65535, but do not use the number of any common service port. The default is 8080, which is a common alternate for HTTP.

4. Click **Apply** to have your changes take effect.
5. When accessing your firewall from the Internet, the Secure Sockets Layer (SSL) will be enabled. You will enter *https://* and type your firewall's WAN IP address into your browser, followed by a colon (:) and the custom port number. For example, if your WAN IP address is 134.177.0.123 and you use port number 8080, type the following in your browser:

   https://134.177.0.123:8080

   If you do not use the SSL *https://address*, but rather use *http://address*, the FVS318v3 will automatically attempt to redirect to *https://address.*

   Note: The first time you remotely connect the FVS318v3 with a browser via SSL, you may get a message regarding the SSL certificate. If you are using a Windows computer with Internet Explorer 5.5 or higher, simply click **Yes** to accept the certificate.

Tip: If you are using a dynamic DNS service such as TZO, you can always identify the IP address of your FVS318v3 by running TRACERT from the Windows Start menu Run option. For example, type **tracert yourFVS318v3.mynetgear.net** and you will see the IP address your ISP assigned to the FVS318v3.

Chapter 9
Troubleshooting

This chapter gives information about troubleshooting your FVS318v3 ProSafe VPN Firewall. After each problem description, instructions are provided to help you diagnose and solve the problem.

Basic Functioning

After you turn on power to the firewall, the following sequence of events should occur:

1. When power is first applied, verify that the PWR LED is on.
2. After approximately 30 seconds, verify that:
   a. The TEST LED is not lit.
   b. The LAN port LEDs are lit for any local ports that are connected.
   c. The Internet port LED is lit.

   If a port's LED is lit, a link has been established to the connected device. If a LAN port is connected to a 100 Mbps device, verify that the port's LED is green. If the port is 10 Mbps, the LED will be green.

If any of these conditions does not occur, refer to the appropriate following section.

Power LED Not On

If the Power and other LEDs are off when your firewall is turned on:

- Make sure that the power cord is properly connected to your firewall and that the power supply adapter is properly connected to a functioning power outlet.
- Check that you are using the 12 V DC power adapter supplied by NETGEAR for this product.

If the error persists, you have a hardware problem and should contact technical support.

LEDs Never Turn Off

When the firewall is turned on, the LEDs turn on briefly and then turn off. If all the LEDs stay on, there is a fault within the firewall.

If all LEDs are still on one minute after power up:

- Cycle the power to see if the firewall recovers.
- Clear the firewall's configuration to factory defaults. This will set the firewall's IP address to 192.168.0.1. This procedure is explained in "Restoring the Default Configuration and Password" on page 9-7.

If the error persists, you might have a hardware problem and should contact technical support.

LAN or Internet Port LEDs Not On

If either the LAN LEDs or Internet LED do not light when the Ethernet connection is made, check the following:

- Make sure that the Ethernet cable connections are secure at the firewall and at the hub or workstation.
- Make sure that power is turned on to the connected hub or workstation.
- Be sure you are using the correct cable:

  When connecting the firewall's Internet port to a cable or DSL modem, use the cable that was supplied with the cable or DSL modem. This cable could be a standard straight-through Ethernet cable or an Ethernet crossover cable.

Troubleshooting the Web Configuration Interface

If you are unable to access the firewall's Web Configuration interface from a PC on your local network, check the following:

- Check the Ethernet connection between the PC and the firewall as described in the previous section.
- Make sure your PC's IP address is on the same subnet as the firewall. If you are using the recommended addressing scheme, your PC's address should be in the range of 192.168.0.2 to 192.168.0.254.

  Note: If your PC's IP address is shown as 169.254.x.x: Recent versions of Windows and MacOS will generate and assign an IP address if the computer cannot reach a DHCP server. These auto-generated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the PC to the firewall and reboot your PC.
- If your firewall's IP address has been changed and you don't know the current IP address, clear the firewall's configuration to factory defaults. This will set the firewall's IP address to 192.168.0.1. This procedure is explained in "Restoring the Default Configuration and Password" on page 9-7.
- Make sure your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to be sure the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure you are using the correct login information. The factory default login name is **admin** and the password is **password**. Make sure that CAPS LOCK is off when entering this information.

If the firewall does not save changes you have made in the Web Configuration Interface, check the following:

- When entering configuration settings, be sure to click the **Apply** button before moving to another menu or tab, or your changes are lost.
- Click the **Refresh** or **Reload** button in the Web browser. The changes may have occurred, but the Web browser may be caching the old configuration.

Troubleshooting the ISP Connection

If your firewall is unable to access the Internet, you should first determine whether the firewall is able to obtain a WAN IP address from the ISP. Unless you have been assigned a static IP address, your firewall must request an IP address from the ISP. You can determine whether the request was successful using the Web Configuration Manager.

To check the WAN IP address:

1. Launch your browser and select an external site such as http://www.netgear.com
2. Access the main menu of the firewall's configuration at *http://192.168.0.1*
3. Under the Maintenance heading, select **Router Status**
4. Check that an IP address is shown for the WAN Port
   If 0.0.0.0 is shown, your firewall has not obtained an IP address from your ISP.

If your firewall is unable to obtain an IP address from the ISP, you may need to force your cable or DSL modem to recognize your new firewall by performing the following procedure:

1. Turn off power to the cable or DSL modem.
2. Turn off power to your firewall.
3. Wait five minutes and reapply power to the cable or DSL modem.
4. When the modem's LEDs indicate that it has reacquired sync with the ISP, reapply power to your firewall.

If your firewall is still unable to obtain an IP address from the ISP, the problem may be one of the following:

- Your ISP may require a login program.
  Ask your ISP whether they require PPP over Ethernet (PPPoE) or some other type of login.
- If your ISP requires a login, you may have incorrectly set the login name and password.
- Your ISP may check for your PC's host name.
  Assign the PC Host Name of your ISP account as the Account Name in the Basic Settings menu.
- Your ISP only allows one Ethernet MAC address to connect to Internet, and may check for your PC's MAC address. In this case:

  Inform your ISP that you have bought a new network device, and ask them to use the firewall's MAC address.

OR

Configure your firewall to spoof your PC's MAC address. This can be done in the Basic Settings menu. Refer to "How to Manually Configure Your Internet Connection" on page 3-12.

If your firewall can obtain an IP address, but your PC is unable to load any Web pages from the Internet:

- Your PC may not recognize any DNS server addresses.

  A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP will provide the addresses of one or two DNS servers for your use. Alternatively, you may configure your PC manually with DNS addresses, as explained in your operating system documentation.

- Your PC may not have the firewall configured as its TCP/IP gateway.

  If your PC obtains its information from the firewall by DHCP, reboot the PC and verify the gateway address.

Troubleshooting a TCP/IP Network Using a Ping Utility

Most TCP/IP terminal devices and firewalls contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. Troubleshooting a TCP/IP network is made very easy by using the ping utility in your PC or workstation.

Testing the LAN Path to Your Firewall

You can ping the firewall from your PC to verify that the LAN path to your firewall is set up correctly.

To ping the firewall from a PC running Windows 95 or later:

1. From the Windows toolbar, click the **Start** button and select **Run**.
2. In the field provided, type ping followed by the IP address of the firewall, as in this example:

   ping 192.168.0.1

3. Click on **OK**.

   You should see a message like this one:

   Pinging <IP address> with 32 bytes of data

If the path is working, you see this message:

```
Reply from < IP address >: bytes=32 time=NN ms TTL=xxx
```

If the path is not working, you see this message:

```
Request timed out
```

If the path is not functioning correctly, you could have one of the following problems:

- Wrong physical connections
  - — Make sure the LAN port LED is on. If the LED is off, follow the instructions in "LAN or Internet Port LEDs Not On" on page 9-2".
  - — Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and firewall.
- Wrong network configuration
  - — Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.
  - — Verify that the IP address for your firewall and your workstation are correct and that the addresses are on the same subnet.

Testing the Path from Your PC to a Remote Device

After verifying that the LAN path works correctly, test the path from your PC to a remote device. From the Windows run menu, type:

PING -n 10 <*IP address*>

where <*IP address*> is the IP address of a remote device such as your ISP's DNS server.

If the path is functioning correctly, replies as in the previous section are displayed. If you do not receive replies:

- — Check that your PC has the IP address of your firewall listed as the default gateway. If the IP configuration of your PC is assigned by DHCP, this information will not be visible in your PC's Network Control Panel. Verify that the IP address of the firewall is listed as the default gateway.
- — Check to see that the network address of your PC (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- — Check that your cable or DSL modem is connected and functioning.

— If your ISP assigned a host name to your PC, enter that host name as the Account Name in the Basic Settings menu.

— Your ISP could be rejecting the Ethernet MAC addresses of all but one of your PCs. Many broadband ISPs restrict access by only allowing traffic from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single PC connected to that modem. If this is the case, you must configure your firewall to "clone" or "spoof" the MAC address from the authorized PC. Refer to "How to Manually Configure Your Internet Connection" on page 3-12.

Restoring the Default Configuration and Password

This section explains how to restore the factory default configuration settings, changing the firewall's administration password to **password** and the IP address to 192.168.0.1. You can erase the current configuration and restore factory defaults in two ways:

- Use the Erase function of the firewall (see "Erasing the Configuration" on page 7-8).
- Use the **Reset** button on the rear panel of the firewall. Use this method for cases when the administration password or IP address are not known.

1. Press and hold the **Reset** button until the Test LED turns on and begins blinking (about 10 seconds).
2. Release the **Reset** button and wait for the firewall to reboot.

Problems with Date and Time

The E-Mail menu in the Content Filtering section displays the current date and time of day. The FVS318v3 VPN Firewall uses the Network Time Protocol (NTP) to obtain the current time from one of several Network Time Servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include:

- Date shown is January 1, 2000. Cause: The firewall has not yet successfully reached a Network Time Server. Check that your Internet access settings are configured correctly. If you have just completed configuring the firewall, wait at least five minutes and check the date and time again.
- Time is off by one hour. Cause: The firewall does not automatically sense Daylight Savings Time. In the E-Mail menu, check or uncheck the box marked **Adjust for Daylight Savings Time**.

Appendix A
Technical Specifications

This appendix provides technical specifications for the FVS318v3 ProSafe VPN Firewall.

Network Protocol and Standards Compatibility

Data and Routing Protocols:	TCP/IP, RIP-1, RIP-2, DHCP PPP over Ethernet (PPPoE)

Power Adapter

North America:	120V, 60 Hz, input
United Kingdom, Australia:	240V, 50 Hz, input
Europe:	230V, 50 Hz, input
Japan:	100V, 50/60 Hz, input
All regions (output):	12 V DC @ 1.2 A output, 18W maximum

Physical Specifications

Dimensions:	39.6 x 254 x 178 mm (1.6 x 10 x 7 in)
Weight:	1.23 kg (2.72 lb)

Environmental Specifications

Operating temperature:	0° to 40° C (32º to 104º F)
Operating humidity:	90% maximum relative humidity, noncondensing

Electromagnetic Emissions	
Meets requirements of:	FCC Part 15 Class B
	VCCI Class B
	EN 55 022 (CISPR 22), Class B
Interface Specifications	
LAN:	10BASE-T or 100BASE-Tx, RJ-45
WAN:	10BASE-T or 100BASE-Tx, RJ-45

Appendix B
Network, Routing, and Firewall Basics

This chapter provides an overview of IP networks, routing, and networking.

Related Publications

As you read this document, you may be directed to various RFC documents for further information. An RFC is a Request For Comment (RFC) published by the Internet Engineering Task Force (IETF), an open organization that defines the architecture and operation of the Internet. The RFC documents outline and define the standard protocols and procedures for the Internet. The documents are listed on the World Wide Web at *www.ietf.org* and are mirrored and indexed at many other sites worldwide.

Basic Router Concepts

Large amounts of bandwidth can be provided easily and relatively inexpensively in a local area network (LAN). However, providing high bandwidth between a local network and the Internet can be very expensive. Because of this expense, Internet access is usually provided by a slower-speed wide-area network (WAN) link such as a cable or DSL modem. In order to make the best use of the slower WAN link, a mechanism must be in place for selecting and transmitting only the data traffic meant for the Internet. The function of selecting and forwarding this data is performed by a router.

What is a Router?

A router is a device that forwards traffic between networks based on network layer information in the data and on routing tables maintained by the router. In these routing tables, a router builds up a logical picture of the overall network by gathering and exchanging information with other routers in the network. Using this information, the router chooses the best path for forwarding network traffic.

Routers vary in performance and scale, number of routing protocols supported, and types of physical WAN connection they support. The FVS318v3 ProSafe VPN Firewall is a small office router that routes the IP protocol over a single-user broadband connection.

Routing Information Protocol

One of the protocols used by a router to build and maintain a picture of the network is the Routing Information Protocol (RIP). Using RIP, routers periodically update one another and check for changes to add to the routing table.

The FVS318v3 VPN Firewall supports both the older RIP-1 and the newer RIP-2 protocols. Among other improvements, RIP-2 supports subnet and multicast protocols. RIP is not required for most home applications.

IP Addresses and the Internet

Because TCP/IP networks are interconnected across the world, every machine on the Internet must have a unique address to make sure that transmitted data reaches the correct destination. Blocks of addresses are assigned to organizations by the Internet Assigned Numbers Authority (IANA). Individual users and small organizations may obtain their addresses either from the IANA or from an Internet service provider (ISP). You can contact IANA at www.iana.org.

The Internet Protocol (IP) uses a 32-bit address structure. The address is usually written in dot notation (also called dotted-decimal notation), in which each group of eight bits is written in decimal form, separated by decimal points.

For example, the following binary address:

```
11000011  00100010  00001100  00000111
```

is normally written as:

```
195.34.12.7
```

The latter version is easier to remember and easier to enter into your computer.

In addition, the 32 bits of the address are subdivided into two parts. The first part of the address identifies the network, and the second part identifies the host node or station on the network. The dividing point may vary depending on the address range and the application.

There are five standard classes of IP addresses. These address classes have different ways of determining the network and host sections of the address, allowing for different numbers of hosts on a network. Each address type begins with a unique bit pattern, which is used by the TCP/IP software to identify the address class. After the address class has been determined, the software can correctly identify the host section of the address. The follow figure shows the three main address classes, including network and host sections of the address for each address type.

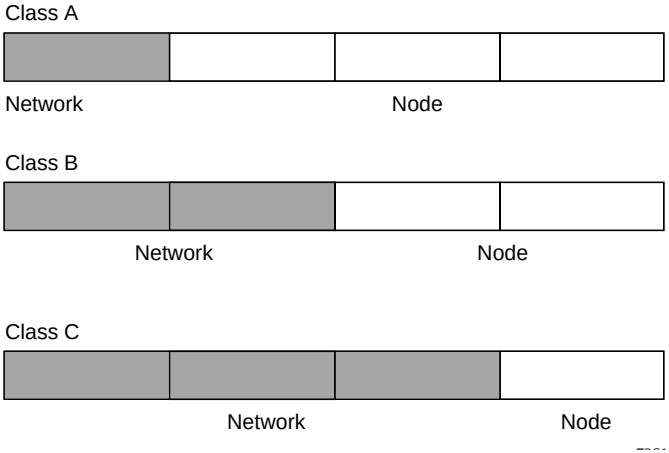


Figure B-1: Three Main Address Classes

The five address classes are:

- Class A
  Class A addresses can have up to 16,777,214 hosts on a single network. They use an eight-bit network number and a 24-bit node number. Class A addresses are in this range:

  `1.x.x.x to 126.x.x.x.`

- Class B
  Class B addresses can have up to 65,354 hosts on a network. A Class B address uses a 16-bit network number and a 16-bit node number. Class B addresses are in this range:

  `128.1.x.x to 191.254.x.x.`

- Class C
  Class C addresses can have 254 hosts on a network. Class C addresses use 24 bits for the network address and eight bits for the node. They are in this range:

  `192.0.1.x to 223.255.254.x.`

- Class D
  Class D addresses are used for multicasts (messages sent to many hosts). Class D addresses are in this range:

  `224.0.0.0 to 239.255.255.255.`

- Class E
  Class E addresses are for experimental use.

This addressing structure allows IP addresses to uniquely identify each physical network and each node on each physical network.

For each unique value of the network portion of the address, the base address of the range (host address of all zeros) is known as the network address and is not usually assigned to a host. Also, the top address of the range (host address of all ones) is not assigned, but is used as the broadcast address for simultaneously sending a packet to all hosts with the same network address.

Netmask

In each of the address classes previously described, the size of the two parts (network address and host address) is implied by the class. This partitioning scheme can also be expressed by a netmask associated with the IP address. A netmask is a 32-bit quantity that, when logically combined (using an AND operator) with an IP address, yields the network address. For instance, the netmasks for Class A, B, and C addresses are 255.0.0.0, 255.255.0.0, and 255.255.255.0, respectively.

For example, the address 192.168.170.237 is a Class C IP address whose network portion is the upper 24 bits. When combined (using an AND operator) with the Class C netmask, as shown here, only the network portion of the address remains:

```
11000000  10101000  10101010  11101101 (192.168.170.237)
```

combined with:

```
11111111  11111111  11111111  00000000 (255.255.255.0)
```

Equals:

```
11000000  10101000  10101010  00000000 (192.168.170.0)
```

As a shorter alternative to dotted-decimal notation, the netmask may also be expressed in terms of the number of ones from the left. This number is appended to the IP address, following a backward slash (/), as "/n." In the example, the address could be written as 192.168.170.237/24, indicating that the netmask is 24 ones followed by 8 zeros.

Subnet Addressing

By looking at the addressing structures, you can see that even with a Class C address, there are a large number of hosts per network. Such a structure is an inefficient use of addresses if each end of a routed link requires a different network number. It is unlikely that the smaller office LANs would have that many devices. You can resolve this problem by using a technique known as subnet addressing.

Subnet addressing allows us to split one IP network address into smaller multiple physical networks known as subnetworks. Some of the node numbers are used as a subnet number instead. A Class B address gives us 16 bits of node numbers translating to 64,000 nodes. Most organizations do not use 64,000 nodes, so there are free bits that can be reassigned. Subnet addressing makes use of those bits that are free, as shown below.

Figure B-2: Example of Subnetting a Class B Address

A Class B address can be effectively translated into multiple Class C addresses. For example, the IP address of 172.16.0.0 is assigned, but node addresses are limited to 255 maximum, allowing eight extra bits to use as a subnet address. The IP address of 172.16.97.235 would be interpreted as IP network address 172.16, subnet number 97, and node number 235. In addition to extending the number of addresses available, subnet addressing provides other benefits. Subnet addressing allows a network manager to construct an address scheme for the network by using different subnets for other geographical locations in the network or for other departments in the organization.

Although the preceding example uses the entire third octet for a subnet address, note that you are not restricted to octet boundaries in subnetting. To create more network numbers, you need only shift some bits from the host address to the network address. For instance, to partition a Class C network number (192.68.135.0) into two, you shift one bit from the host address to the network address. The new netmask (or subnet mask) is 255.255.255.128. The first subnet has network number 192.68.135.0 with hosts 192.68.135.1 to 129.68.135.126, and the second subnet has network number 192.68.135.128 with hosts 192.68.135.129 to 192.68.135.254.

Note: The number 192.68.135.127 is not assigned because it is the broadcast address of the first subnet. The number 192.68.135.128 is not assigned because it is the network address of the second subnet.

The following table lists the additional subnet mask bits in dotted-decimal notation. To use the table, write down the original class netmask and replace the 0 value octets with the dotted-decimal value of the additional subnet bits. For example, to partition your Class C network with subnet mask 255.255.255.0 into 16 subnets (4 bits), the new subnet mask becomes 255.255.255.240.

Table B-1. Netmask notation translation table for one octet

Number of Bits	Dotted-Decimal Value
1	128
2	192
3	224
4	240
5	248
6	252
7	254
8	255

The following table displays several common netmask values in both the dotted-decimal and the masklength formats.

Table B-2. Netmask formats

Dotted-Decimal	Masklength
255.0.0.0	/8

Table B-2. Netmask formats

255.255.0.0	/16
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30
255.255.255.254	/31
255.255.255.255	/32

Configure all hosts on a LAN segment to use the same netmask for the following reasons:

- So that hosts recognize local IP broadcast packets

  When a device broadcasts to its segment neighbors, it uses a destination address of the local network address with all ones for the host address. In order for this scheme to work, all devices on the segment must agree on which bits comprise the host address.

- So that a local router or bridge recognizes which addresses are local and which are remote

Private IP Addresses

If your local network is isolated from the Internet (for example, when using NAT), you can assign any IP addresses to the hosts without problems. However, the IANA has reserved the following three blocks of IP addresses specifically for private networks:

```
10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255
```

Choose your private network number from this range. The DHCP server of the FVS318v3 VPN Firewall is preconfigured to automatically assign private addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines explained here. For more information about address assignment, refer to RFC 1597, *Address Allocation for Private Internets*, and RFC 1466, *Guidelines for Management of IP Address Space*. The Internet Engineering Task Force (IETF) publishes RFCs on its Web site at www.ietf.org.

Single IP Address Operation Using NAT

In the past, if multiple PCs on a LAN needed to access the Internet simultaneously, you had to obtain a range of IP addresses from the ISP. This type of Internet account is more costly than a single-address account typically used by a single user with a modem, rather than a router. The FVS318v3 VPN Firewall employs an address-sharing method called Network Address Translation (NAT). This method allows several networked PCs to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your ISP.

The router accomplishes this address sharing by translating the internal LAN IP addresses to a single address that is globally unique on the Internet. The internal LAN IP addresses can be either private addresses or registered addresses. For more information about IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT)*.

The following figure illustrates a single IP address operation.

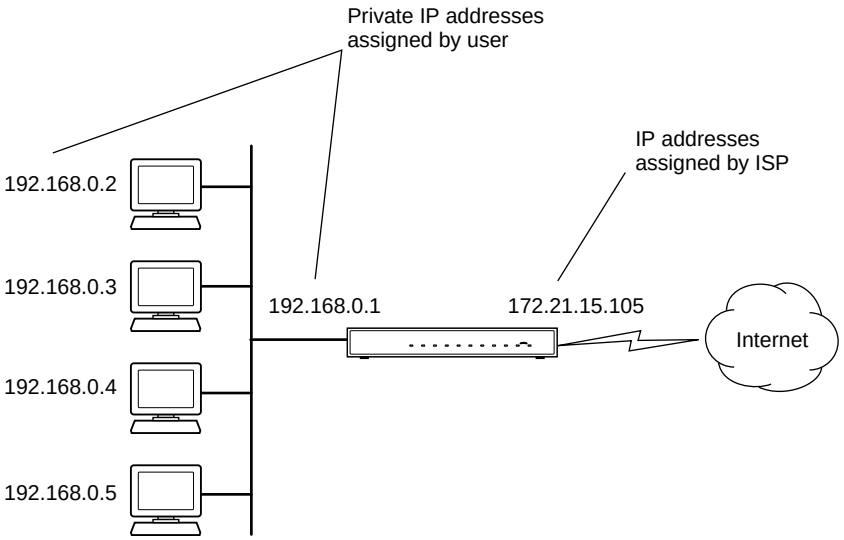


Figure B-3: Single IP Address Operation Using NAT

This scheme offers the additional benefit of firewall-like protection because the internal LAN addresses are not available to the Internet through the translated connection. All incoming inquiries are filtered out by the router. This filtering can prevent intruders from probing your system. However, using port forwarding, you can allow one PC (for example, a Web server) on your local network to be accessible to outside users.

MAC Addresses and Address Resolution Protocol

An IP address alone cannot be used to deliver data from one LAN device to another. To send data between LAN devices, you must convert the IP address of the destination device to its media access control (MAC) address. Each device on an Ethernet network has a unique MAC address, which is a 48-bit number assigned to each device by the manufacturer. The technique that associates the IP address with a MAC address is known as address resolution. Internet Protocol uses the Address Resolution Protocol (ARP) to resolve MAC addresses.

If a device sends data to another station on the network and the destination MAC address is not yet recorded, ARP is used. An ARP request is broadcast onto the network. All stations on the network receive and read the request. The destination IP address for the chosen station is included as part of the message so that only the station with this IP address responds to the ARP request. All other stations discard the request.

Related Documents

The station with the correct IP address responds with its own MAC address directly to the sending device. The receiving station provides the transmitting station with the required destination MAC address. The IP address data and MAC address data for each station are held in an ARP table. The next time data is sent, the address can be obtained from the address information in the table.

For more information about address assignment, refer to the IETF documents RFC 1597, *Address Allocation for Private Internets,* and RFC 1466, *Guidelines for Management of IP Address Space*.

For more information about IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT)*.

Domain Name Server

Many of the resources on the Internet can be addressed by simple descriptive names such as *www.NETGEAR.com*. This addressing is very helpful at the application level, but the descriptive name must be translated to an IP address in order for a user to actually contact the resource. Just as a telephone directory maps names to phone numbers, or as an ARP table maps IP addresses to MAC addresses, a domain name system (DNS) server maps descriptive names of network resources to IP addresses.

When a PC accesses a resource by its descriptive name, it first contacts a DNS server to obtain the IP address of the resource. The PC sends the desired message using the IP address. Many large organizations, such as ISPs, maintain their own DNS servers and allow their customers to use the servers to look up addresses.

IP Configuration by DHCP

When an IP-based local area network is installed, each PC must be configured with an IP address. If the PCs need to access the Internet, they should also be configured with a gateway address and one or more DNS server addresses. As an alternative to manual configuration, there is a method by which each PC on the network can automatically obtain this configuration information. A device on the network may act as a Dynamic Host Configuration Protocol (DHCP) server. The DHCP server stores a list or pool of IP addresses, along with other information (such as gateway and DNS addresses) that it may assign to the other devices on the network. The FVS318v3 VPN Firewall has the capacity to act as a DHCP server.

The FVS318v3 VPN Firewall also functions as a DHCP client when connecting to the ISP. The firewall can automatically obtain an IP address, subnet mask, DNS server addresses, and a gateway address if the ISP provides this information by DHCP.

Internet Security and Firewalls

When your LAN connects to the Internet through a router, an opportunity is created for outsiders to access or disrupt your network. A NAT router provides some protection because by the very nature of the process, the network behind the router is shielded from access by outsiders on the Internet. However, there are methods by which a determined hacker can possibly obtain information about your network or at the least can disrupt your Internet access. A greater degree of protection is provided by a firewall router.

What is a Firewall?

A firewall is a device that protects one network from another, while allowing communication between the two. A firewall incorporates the functions of the NAT router, while adding features for dealing with a hacker intrusion or attack. Several known types of intrusion or attack can be recognized when they occur. When an incident is detected, the firewall can log details of the attempt, and can optionally send email to an administrator notifying them of the incident. Using information from the log, the administrator can take action with the ISP of the hacker. In some types of intrusions, the firewall can fend off the hacker by discarding all further packets from the hacker's IP address for a period of time.

Stateful Packet Inspection

Unlike simple Internet sharing routers, a firewall uses a process called stateful packet inspection to ensure secure firewall filtering to protect your network from attacks and intrusions. Since user-level applications such as FTP and Web browsers can create complex patterns of network traffic, it is necessary for the firewall to analyze groups of network connection states. Using Stateful Packet Inspection, an incoming packet is intercepted at the network layer and then analyzed for state-related information associated with all network connections. A central cache within the firewall keeps track of the state information associated with all network connections. All traffic passing through the firewall is analyzed against the state of these connections in order to determine whether or not it will be allowed to pass through or rejected.

Denial of Service Attack

A hacker may be able to prevent your network from operating or communicating by launching a Denial of Service (DoS) attack. The method used for such an attack can be as simple as merely flooding your site with more requests than it can handle. A more sophisticated attack may attempt to exploit some weakness in the operating system used by your router or gateway. Some operating systems can be disrupted by simply sending a packet with incorrect length information.

Ethernet Cabling

Although Ethernet networks originally used thick or thin coaxial cable, most installations currently use unshielded twisted pair (UTP) cabling. The UTP cable contains eight conductors, arranged in four twisted pairs, and terminated with an RJ45 type connector. A normal straight-through UTP Ethernet cable follows the EIA568B standard wiring as described below in Table B-3.

Table B-3. UTP Ethernet cable wiring, straight-through

Pin	Wire color	Signal
1	Orange/White	Transmit (Tx) +
2	Orange	Transmit (Tx) -
3	Green/White	Receive (Rx) +
4	Blue	
5	Blue/White	
6	Green	Receive (Rx) -
7	Brown/White	
8	Brown	

Category 5 Cable Quality

Category 5 distributed cable that meets ANSI/EIA/TIA-568-A building wiring standards can be a maximum of 328 feet (ft.) or 100 meters (m) in length, divided as follows:

20 ft. (6 m) between the hub and the patch panel (if used)

295 ft. (90 m) from the wiring closet to the wall outlet

10 ft. (3 m) from the wall outlet to the desktop device

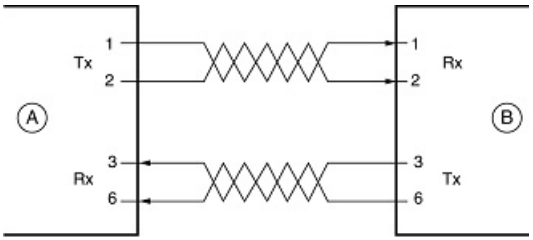
The patch panel and other connecting hardware must meet the requirements for 100 Mbps operation (Category 5). Only 0.5 inch (1.5 cm) of untwist in the wire pair is allowed at any termination point.

A twisted pair Ethernet network operating at 10 Mbits/second (10BASE-T) will often tolerate low quality cables, but at 100 Mbits/second (10BASE-Tx) the cable must be rated as Category 5, or Cat 5, by the Electronic Industry Association (EIA). This rating will be printed on the cable jacket. A Category 5 cable will meet specified requirements regarding loss and crosstalk. In addition, there are restrictions on maximum cable length for both 10 and 100 Mbits/second networks.

Inside Twisted Pair Cables

For two devices to communicate, the transmitter of each device must be connected to the receiver of the other device. The crossover function is usually implemented internally as part of the circuitry in the device. Computers and workstation adapter cards are usually media-dependent interface ports, called MDI or uplink ports. Most repeaters and switch ports are configured as media-dependent interfaces with built-in crossover ports, called MDI-X or normal ports. Auto Uplink technology automatically senses which connection, MDI or MDI-X, is needed and makes the right connection.

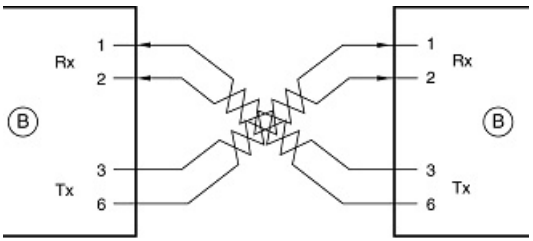
Figure B-4 illustrates straight-through twisted pair cable.



Key:
A = UPLINK OR MDI PORT (as on a PC)
B = Normal or MDI-X port (as on a hub or switch)
1, 2, 3, 6 = Pin numbers

Figure B-4: Straight-through twisted-pair cable

Figure B-5 illustrates crossover twisted pair cable.



Key:
B = Normal or MDI-X port (as on a hub or switch)
1, 2, 3, 6 = Pin numbers

Figure B-5: Crossover twisted-pair cable

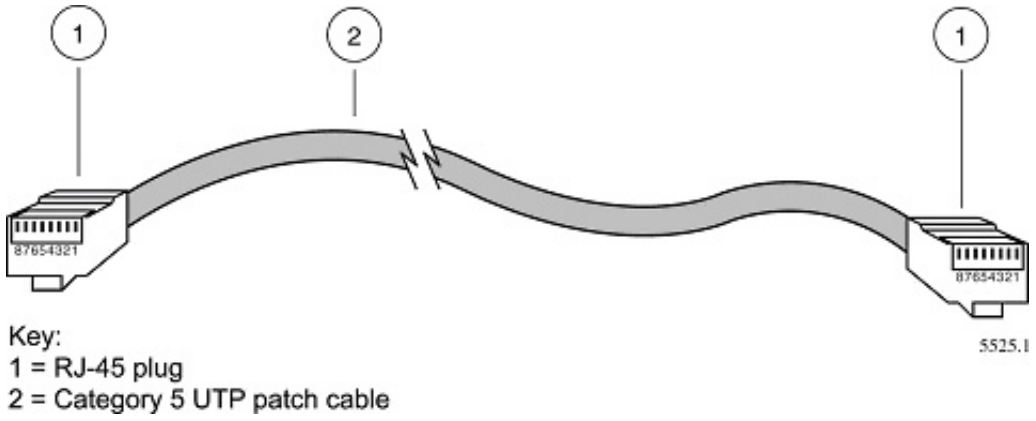


Figure B-6: Category 5 UTP cable with male RJ-45 plug at each end

Note: Flat “silver satin” telephone cable may have the same RJ-45 plug. However, using telephone cable results in excessive collisions, causing the attached port to be partitioned or disconnected from the network.

Uplink Switches, Crossover Cables, and MDI/MDIX Switching

In the wiring table above, the concept of transmit and receive are from the perspective of the PC, which is wired as Media Dependant Interface (MDI). In this wiring, the PC transmits on pins 1 and 2. At the hub, the perspective is reversed, and the hub receives on pins 1 and 2. This wiring is referred to as Media Dependant Interface - Crossover (MDI-X).

When connecting a PC to a PC, or a hub port to another hub port, the transmit pair must be exchanged with the receive pair. This exchange is done by one of two mechanisms. Most hubs provide an Uplink switch which will exchange the pairs on one port, allowing that port to be connected to another hub using a normal Ethernet cable. The second method is to use a crossover cable, which is a special cable in which the transmit and receive pairs are exchanged at one of the two cable connectors. Crossover cables are often unmarked as such, and must be identified by comparing the two connectors. Since the cable connectors are clear plastic, it is easy to place them side by side and view the order of the wire colors on each. On a straight-through cable, the color order will be the same on both connectors. On a crossover cable, the orange and blue pairs will be exchanged from one connector to the other.

The FVS318v3 VPN Firewall incorporates Auto Uplink™ technology (also called MDI/MDIX). Each LOCAL Ethernet port will automatically sense whether the Ethernet cable plugged into the port should have a normal connection (e.g. connecting to a PC) or an uplink connection (e.g. connecting to a router, switch, or hub). That port will then configure itself to the correct configuration. This feature also eliminates the need to worry about crossover cables, as Auto Uplink™ will accommodate either type of cable to make the right connection.

Appendix C
Virtual Private Networking

There have been many improvements in the Internet including Quality of Service, network performance, and inexpensive technologies, such as DSL. But one of the most important advances has been in Virtual Private Networking (VPN) Internet Protocol security (IPSec). IPSec is one of the most complete, secure, and commercially available, standards-based protocols developed for transporting data.

What is a VPN?

A VPN is a shared network where private data is segmented from other traffic so that only the intended recipient has access. The term VPN was originally used to describe a secure connection over the Internet. Today, however, VPN is also used to describe private networks, such as Frame Relay, Asynchronous Transfer Mode (ATM), and Multiprotocol Label Switching (MPLS).

A key aspect of data security is that the data flowing across the network is protected by encryption technologies. Private networks lack data security; so data attackers can tap directly into the network and read the data. IPSec-based VPNs use encryption to provide data security, which increases the network's resistance to data tampering or theft.

IPSec-based VPNs can be created over any type of IP network, including the Internet, Frame Relay, ATM, and MPLS, but only the Internet is ubiquitous and inexpensive.

VPNs are traditionally used for:

- **Intranets:** Intranets connect an organization's locations. These locations range from the headquarters offices, to branch offices, to a remote employee's home. Often this connectivity is used for e-mail and for sharing applications and files. While Frame Relay, ATM, and MPLS accomplish these tasks, the shortcomings of each limits connectivity. The cost of connecting home users is also very expensive compared to Internet-access technologies, such as DSL or cable. Because of this, organizations are moving their networks to the Internet, which is inexpensive, and using IPSec to create these networks.

- **Remote Access:** Remote access enables telecommuters and mobile workers to access e-mail and business applications. A dial-up connection to an organization's modem pool is one method of access for remote workers, but is expensive because the organization must pay the associated long distance telephone and service costs. Remote access VPNs greatly reduce expenses by enabling mobile workers to dial a local Internet connection and then set up a secure IPSec-based VPN communications to their organization.
- **Extranets**: Extranets are secure connections between two or more organizations. Common uses for extranets include supply-chain management, development partnerships, and subscription services. These undertakings can be difficult using legacy network technologies due to connection costs, time delays, and access availability. IPSec-based VPNs are ideal for extranet connections. IPSec-capable devices can be quickly and inexpensively installed on existing Internet connections.

What Is IPSec and How Does It Work?

IPSec is an Internet Engineering Task Force (IETF) standard suite of protocols that provides data authentication, integrity, and confidentiality as data is transferred between communication points across IP networks. IPSec provides data security at the IP packet level. A packet is a data bundle that is organized for transmission across a network, and includes a header and payload (the data in the packet). IPSec emerged as a viable network security standard because enterprises wanted to ensure that data could be securely transmitted over the Internet. IPSec protects against possible security exposures by protecting data while in transit.

IPSec Security Features

IPSec is the most secure method commercially available for connecting network sites. IPSec was designed to provide the following security features when transferring packets across networks:

- **Authentication:** Verifies that the packet received is actually from the claimed sender.
- **Integrity:** Ensures that the contents of the packet did not change in transit.
- **Confidentiality:** Conceals the message content through encryption.

IPSec Components

IPSec contains the following elements:

- **Encapsulating Security Payload (ESP)**: Provides confidentiality, authentication, and integrity.
- **Authentication Header (AH)**: Provides authentication and integrity.
- **Internet Key Exchange (IKE)**: Provides key management and Security Association (SA) management.

Encapsulating Security Payload (ESP)

ESP provides authentication, integrity, and confidentiality, which protect against data tampering and, most importantly, provide message content protection.

IPSec provides an open framework for implementing industry standard algorithms, such as SHA and MD5. The algorithms that IPSec uses produce a unique and unforgeable identifier for each packet, which is a data equivalent of a fingerprint. This fingerprint allows the device to determine if a packet has been tampered with. Furthermore, packets that are not authenticated are discarded and not delivered to the intended receiver.

ESP also provides all encryption services in IPSec. Encryption translates a readable message into an unreadable format to hide the message content. The opposite process, called decryption, translates the message content from an unreadable format to a readable message. Encryption and decryption allows only the sender and the authorized receiver to read the data. In addition, ESP has an option to perform authentication, called ESP authentication. Using ESP authentication, ESP provides authentication and integrity for the payload and not for the IP header.

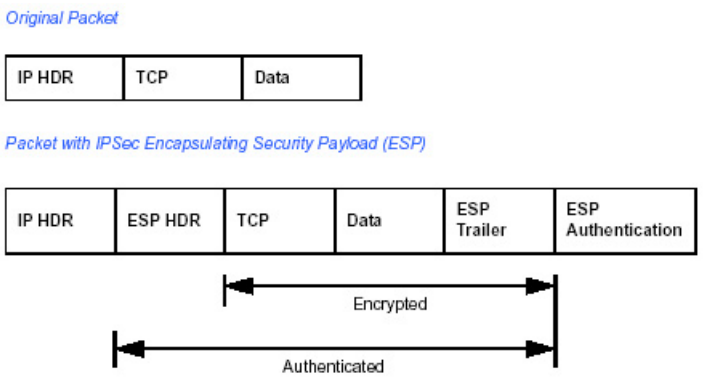


Figure C-1: Original packet and packet with IPSec Encapsulated Security Payload

The ESP header is inserted into the packet between the IP header and any subsequent packet contents. However, because ESP encrypts the data, the payload is changed. ESP does not encrypt the ESP header, nor does it encrypt the ESP authentication.

Authentication Header (AH)

AH provides authentication and integrity, which protect against data tampering, using the same algorithms as ESP. AH also provides optional anti-replay protection, which protects against unauthorized retransmission of packets. The authentication header is inserted into the packet between the IP header and any subsequent packet contents. The payload is not touched.

Although AH protects the packet's origin, destination, and contents from being tampered with, the identity of the sender and receiver is known. In addition, AH does not protect the data's confidentiality. If data is intercepted and only AH is used, the message contents can be read. ESP protects data confidentiality. For added protection in certain cases, AH and ESP can be used together. In the following table, IP HDR represents the IP header and includes both source and destination IP addresses.

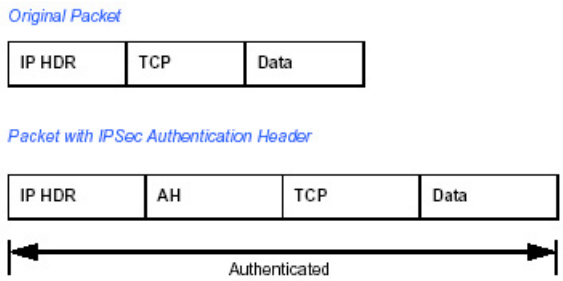


Figure C-2: Original packet and packet with IPSec Authentication Header

IKE Security Association

IPSec introduces the concept of the Security Association (SA). An SA is a logical connection between two devices transferring data. An SA provides data protection for unidirectional traffic by using the defined IPSec protocols. An IPSec tunnel typically consists of two unidirectional SAs, which together provide a protected, full-duplex data channel.

The SAs allow an enterprise to control exactly which resources may communicate securely, according to security policy. To do this an enterprise can set up multiple SAs to enable multiple secure VPNs, as well as define SAs within the VPN to support different departments and business partners.

Mode

SAs operate using modes. A mode is the method in which the IPSec protocol is applied to the packet. IPSec can be used in tunnel mode or transport mode. Typically, the tunnel mode is used for gateway-to-gateway IPSec tunnel protection, while transport mode is used for host-to-host IPSec tunnel protection. A gateway is a device that monitors and manages incoming and outgoing network traffic and routes the traffic accordingly. A host is a device that sends and receives network traffic.

- **Transport Mode:** The transport mode IPSec implementation encapsulates only the packet's payload. The IP header is not changed. After the packet is processed with IPSec, the new IP packet contains the old IP header (with the source and destination IP addresses unchanged) and the processed packet payload. Transport mode does not shield the information in the IP header; therefore, an attacker can learn where the packet is coming from and where it is going. The packet diagrams in Figure C-1 and Figure C-2 show a packet in transport mode.
- **Tunnel Mode:** The tunnel mode IPSec implementation encapsulates the entire IP packet. The entire packet becomes the payload of the packet that is processed with IPSec. A new IP header is created that contains the two IPSec gateway addresses. The gateways perform the encapsulation and decapsulation on behalf of the hosts. Tunnel mode ESP prevents an attacker from analyzing the data and deciphering it, as well as knowing who the packet is from and where it is going.

Note: AH and ESP can be used in both transport mode or tunnel mode.

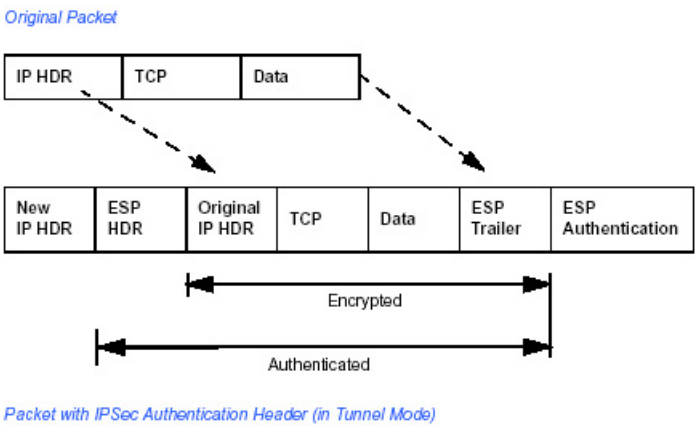


Figure C-3: Original packet and packet with IPSec ESP in Tunnel mode

Key Management

IPSec uses the Internet Key Exchange (IKE) protocol to facilitate and automate the SA setup and the exchange of keys between parties transferring data. Using keys ensures that only the sender and receiver of a message can access it.

IPSec requires that keys be re-created, or refreshed, frequently so that the parties can communicate securely with each other. IKE manages the process of refreshing keys; however, a user can control the key strength and the refresh frequency. Refreshing keys on a regular basis ensures data confidentiality between sender and receiver.

Understand the Process Before You Begin

This appendix provides case studies on how to configure a secure IPSec VPN tunnels. This document assumes the reader has a working knowledge of NETGEAR management systems.

NETGEAR is a member of the VPN Consortium, a group formed to facilitate IPSec VPN vendor interoperability. The VPN Consortium has developed specific scenarios to aid system administrators in the often confusing process of connecting two different vendor implementations of the IPSec standard. The case studies in this TechNote follow the addressing and configuration mechanics defined by the VPN Consortium. Additional information regarding inter-vendor interoperability may be found at *http://www.vpnc.org/interop.html*.

It is a good idea to gather all the necessary information required to establish a VPN before you begin the configuration process. You should understand whether the firmware is up to date, all of the addresses that will be necessary, and all of the parameters that need to be set on both sides. Try to understand any incompatibilities before you begin, so that you minimize any potential complications which may arise from normal firewall or WAN processes.

If you are not a full-time system administrator, it is a good idea to familiarize yourself with the mechanics of a VPN as described in this appendix. Other good sources include:

- The NETGEAR VPN Tutorial – *http://www.netgear.com/planetvpn/pvpn_2.html*
- The VPN Consortium – *http://www.vpnc.org/*
- The VPN bibliography in “Additional Reading” on page C-11.

VPN Process Overview

Even though IPSec is standards-based, each vendor has its own set of terms and procedures for implementing the standard. Because of these differences, it may be a good idea to review some of the terms and the generic processes for connecting two gateways before diving into to the specifics.

Network Interfaces and Addresses

The VPN gateway is aptly named because it functions as a “gatekeeper” for each of the computers connected on the Local Area Network behind it.

In most cases, each gateway will have a public facing address (WAN side) and a private facing address (LAN side). These addresses are referred to as the network interface in documentation regarding the construction of VPN communication.

Interface Addressing

This example uses addresses provided the VPN Consortium. However, when you set up your own equipment, you will be using addresses specific to the devices that you are attempting to connect via IPSec VPN.

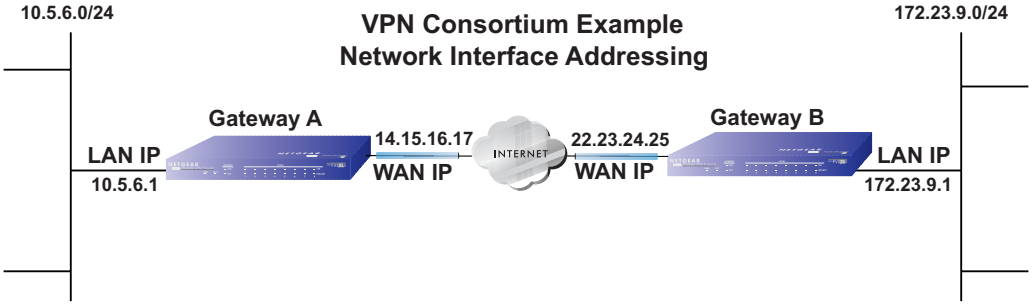


Figure C-4: VPN Consortium example network interface addressing

Make sure the addresses do not overlap or conflict. That is, each set of addresses should be separate and distinct.

Table C-1. WAN (Internet/public) and LAN (internal/private) addressing

Gateway	LAN or WAN	VPNC Example Address
Gateway A	LAN (Private)	10.5.6.1
Gateway A	WAN (Public)	14.15.16.17
Gateway B	LAN (Private)	22.23.24.25
Gateway B	WAN (Public)	172.23.9.1

You need to know the subnet mask of both gateway LAN Connections. Refer to Appendix A, "Technical Specifications" to gather the necessary address and subnet mask information to aid in the configuration and troubleshooting process.

Table C-2. Subnet addressing

Gateway	LAN or WAN	Interface Name	Example Subnet Mask
Gateway A	LAN (Private)	Subnet Mask A	255.255.255.0
Gateway B	LAN (Private)	Subnet Mask B	255.255.255.0

Firewalls

It is important to understand that many gateways are also firewalls. VPN tunnels cannot function properly if firewall settings disallow all incoming traffic. Please refer to the firewall instructions for both gateways to understand how to open specific protocols, ports, and addresses that you intend to allow.

VPN Tunnel Between Gateways

A Security Association (SA), frequently called a tunnel, is the set of information that allows two entities (networks, PCs, routers, firewalls, gateways) to trust each other and communicate securely as they pass information over the Internet.

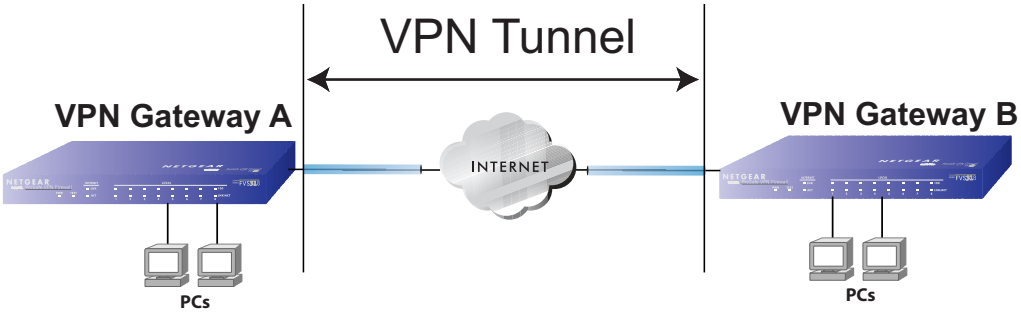


Figure C-5: VPN tunnel Security Associaton (SA)

The SA contains all the information necessary for gateway A to negotiate a secure and encrypted communication stream with gateway B. This communication is often referred to as a "tunnel." The gateways contain this information so that it does not have to be loaded onto every computer connected to the gateways.

Each gateway must negotiate its SA with another gateway using the parameters and processes established by IPSec. As illustrated below, the most common method of accomplishing this process is via the Internet Key Exchange (IKE) protocol which automates some of the negotiation procedures.

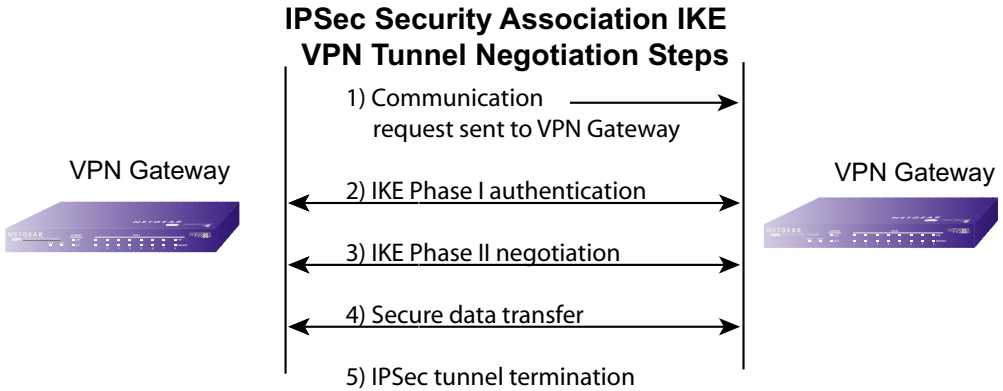

IPSec Security Association IKE
VPN Tunnel Negotiation Steps
VPN Gateway
VPN Gateway
1) Communication request sent to VPN Gateway
2) IKE Phase I authentication
3) IKE Phase II negotiation
4) Secure data transfer
5) IPSec tunnel termination

Figure C-6: IPSec Security Association (SA) negotiation

Or, you can configure your gateways using manual key exchange, which involves manually configuring each paramter on both gateways.

1. **The IPSec software on Host A initiates the IPSec process in an attempt to communicate with Host B.** The two computers then begin the Internet Key Exchange (IKE) process.

2. **IKE Phase I.**
    a. The two parties negotiate the encryption and authentication algorithms to use in the IKE SAs.
    b. The two parties authenticate each other using a predetermined mechanism, such as preshared keys or digital certificates.
    c. A shared master key is generated by the Diffie-Hellman Public key algorithm within the IKE framework for the two parties. The master key is also used in the second phase to derive IPSec keys for the SAs.
3. **IKE Phase II.**
    a. The two parties negotiate the encryption and authentication algorithms to use in the IPSec SAs.
    b. The master key is used to derive the IPSec keys for the SAs. Once the SA keys are created and exchanged, the IPSec SAs are ready to protect user data between the two VPN gateways.
4. **Data transfer.** Data is transferred between IPSec peers based on the IPSec parameters and keys stored in the SA database.
5. **IPSec tunnel termination.** IPSec SAs terminate through deletion or by timing out.

VPNC IKE Security Parameters

Remember that both gateways must have the identical parameters set for the process to work correctly. The settings shown below follow the examples given for Scenario 1 of the VPN Consortium.

VPNC IKE Phase I Parameters

The IKE Phase 1 parameters used:

- Main mode
- TripleDES
- SHA-1
- MODP group 1
- pre-shared secret of "hr5xb84l6aa9r6"
- SA lifetime of 28800 seconds (eight hours)

VPNC IKE Phase II Parameters

The IKE Phase 2 parameters used in Scenario 1 are:

- TripleDES
- SHA-1
- ESP tunnel mode
- MODP group 1
- Perfect forward secrecy for rekeying
- SA lifetime of 28800 seconds (one hour)

Testing and Troubleshooting

Once you have completed the VPN configuration steps you can use PCs, located behind each of the gateways, to ping various addresses on the LAN-side of the other gateway.

You can troubleshoot connections using the VPN status and log details on the Netgear gateway to determine if IKE negotiation is working. Common problems encountered in setting up VPNs include:

- Parameters may be configured differently on Gateway A and Gateway B.
- Two LANs set up with similar or overlapping addressing schemes.
- So many required configuration parameters mean errors such as mistyped information or mismatched parameter selections on either side are more likely to happen.

Additional Reading

- *Building and Managing Virtual Private Networks*, Dave Kosiur, Wiley & Sons; ISBN: 0471295264
- *Firewalls and Internet Security: Repelling the Wily Hacker*, William R. Cheswick and Steven M. Bellovin, Addison-Wesley; ISBN: 0201633574
- *VPNs A Beginners Guide*, John Mains, McGraw Hill; ISBN: 0072191813
- [FF98] Floyd, S., and Fall, K., Promoting the Use of End-to-End Congestion Control in the Internet. IEEE/ACM Transactions on Networking, August 1999.

Relevant RFCs listed numerically:

- [RFC 791] *Internet Protocol DARPA Internet Program Protocol Specification*, Information Sciences Institute, USC, September 1981.
- [RFC 1058] *Routing Information Protocol*, C Hedrick, Rutgers University, June 1988.
- [RFC 1483] *Multiprotocol Encapsulation over ATM Adaptation Layer 5*, Juha Heinanen, Telecom Finland, July 1993.
- [RFC 2401] S. Kent, R. Atkinson, *Security Architecture for the Internet Protocol*, RFC 2401, November 1998.
- [RFC 2407] D. Piper, *The Internet IP Security Domain of Interpretation for ISAKMP*, November 1998.
- [RFC 2474] K. Nichols, S. Blake, F. Baker, D. Black, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*, December 1998.
- [RFC 2475] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, *An Architecture for Differentiated Services*, December 1998.
- [RFC 2481] K. Ramakrishnan, S. Floyd, *A Proposal to Add Explicit Congestion Notification (ECN) to IP*, January 1999.
- [RFC 2408] D. Maughan, M. Schertler, M. Schneider, J. Turner, *Internet Security Association and Key Management Protocol (ISAKMP)*.
- [RFC 2409] D. Harkins, D.Carrel, *Internet Key Exchange* (IKE) protocol.
- [RFC 2401] S. Kent, R. Atkinson, *Security Architecture for the Internet Protocol*.

Appendix D
Preparing Your Network

This appendix describes how to prepare your network to connect to the Internet through the FVS318v3 ProSafe VPN Firewall and how to verify the readiness of broadband Internet service from an Internet service provider (ISP).

Note: If an ISP technician configured your computer during the installation of a broadband modem, or if you configured it using instructions provided by your ISP, you may need to copy the current configuration information for use in the configuration of your firewall. Write down this information before reconfiguring your computers. Refer to "Obtaining ISP Configuration Information for Windows Computers" on page D-19 or "Obtaining ISP Configuration Information for Macintosh Computers" on page D-20 for further information.

Preparing Your Computers for TCP/IP Networking

Computers access the Internet using a protocol called TCP/IP (Transmission Control Protocol/ Internet Protocol). Each computer on your network must have TCP/IP installed and selected as its networking protocol. If a Network Interface Card (NIC) is already installed in your PC, then TCP/ IP is probably already installed as well.

Most operating systems include the software components you need for networking with TCP/IP:

- Windows® 95 or later includes the software components for establishing a TCP/IP network.
- Windows 3.1 does not include a TCP/IP component. You need to purchase a third-party TCP/ IP application package such as NetManage Chameleon.
- Macintosh Operating System 7 or later includes the software components for establishing a TCP/IP network.
- All versions of UNIX or Linux include TCP/IP components. Follow the instructions provided with your operating system or networking software to install TCP/IP on your computer.

In your IP network, each PC and the firewall must be assigned a unique IP addresses. Each PC must also have certain other IP configuration information such as a subnet mask (netmask), a domain name server (DNS) address, and a default gateway address. In most cases, you should install TCP/IP so that the PC obtains its specific network configuration information automatically from a DHCP server during bootup. For a detailed explanation of the meaning and purpose of these configuration items, refer to "Appendix B, "Network, Routing, and Firewall Basics."

The FVS318v3 VPN Firewall is shipped preconfigured as a DHCP server. The firewall assigns the following TCP/IP configuration information automatically when the PCs are rebooted:

- PC or workstation IP addresses—192.168.0.2 through 192.168.0.254
- Subnet mask—255.255.255.0
- Gateway address (the firewall)—192.168.0.1

These addresses are part of the IETF-designated private address range for use in private networks.

Configuring Windows 95, 98, and Me for TCP/IP Networking

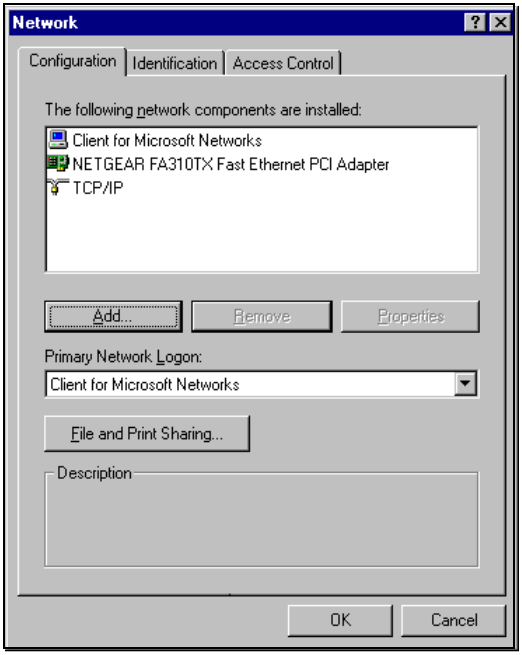
As part of the PC preparation process, you need to manually install and configure TCP/IP on each networked PC. Before starting, locate your Windows CD; you may need to insert it during the TCP/IP installation process.

Install or Verify Windows Networking Components

To install or verify the necessary components for IP networking:

1. On the Windows taskbar, click the **Start** button, point to Settings, and then click **Control Panel**.
2. Double-click the **Network** icon.

   The Network window opens, which displays a list of installed components:



You must have an Ethernet adapter, the TCP/IP protocol, and Client for Microsoft Networks.

Note: It is not necessary to remove any other network components shown in the Network window in order to install the adapter, TCP/IP, or Client for Microsoft Networks.

If you need to install a new adapter, follow these steps:

a. Click the **Add** button.

b. Select **Adapter**, and then click **Add**.

c. Select the manufacturer and model of your Ethernet adapter, and then click **OK**.

If you need TCP/IP:

a. Click the **Add** button.

b. Select **Protocol**, and then click **Add**.

c. Select **Microsoft**.

d. Select **TCP/IP**, and then click **OK**.

If you need Client for Microsoft Networks:

a. Click the **Add** button.

b. Select **Client**, and then click **Add**.

c. Select **Microsoft**.

d. Select **Client for Microsoft Networks**, and then click **OK**.

3. Restart your PC for the changes to take effect.

Enabling DHCP to Automatically Configure TCP/IP Settings

After the TCP/IP protocol components are installed, each PC must be assigned specific information about itself and resources that are available on its network. The simplest way to configure this information is to allow the PC to obtain the information from a DHCP server in the network.

You will find there are many similarities in the procedures for different Windows systems when using DHCP to configure TCP/IP.

The following steps will walk you through the configuration process for each of these versions of Windows.

1

Locate your **Network Neighborhood** icon.

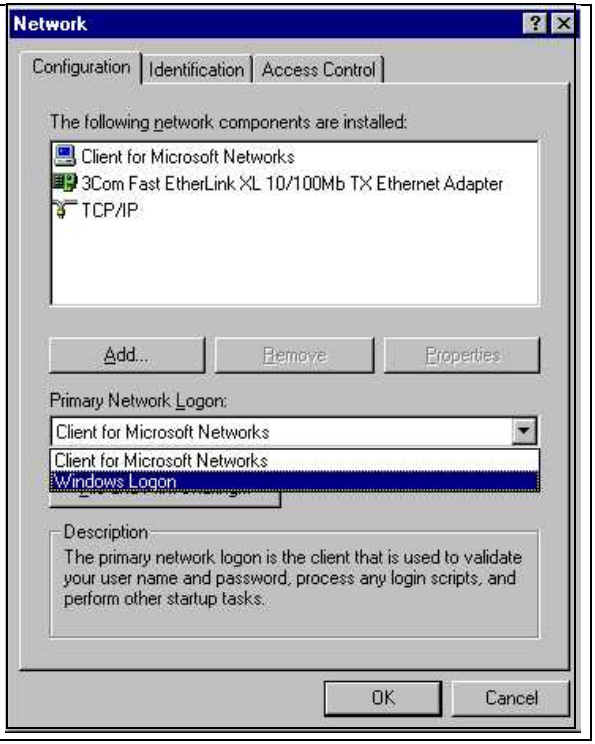
- If the Network Neighborhood icon is on the Windows desktop, position your mouse pointer over it and right-click your mouse button.
- If the icon is not on the desktop,
  - Click **Start** on the task bar located at the bottom left of the window.
  - Choose **Settings**, and then **Control Panel**.
  - Locate the **Network Neighborhood** icon and click on it. This will open the Network panel as shown below.

2

Verify the following settings as shown:

- Client for Microsoft Network exists
- Ethernet adapter is present
- TCP/IP is present
- **Primary Network Logon** is set to Windows logon

Click on the **Properties** button. The following TCP/IP Properties window will display.



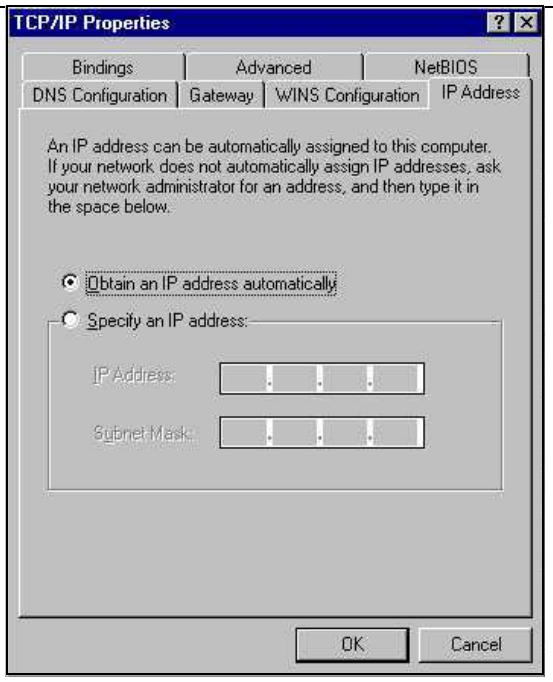
3

- By default, the **IP Address** tab is open on this window.
- Verify the following:

  Obtain an IP address automatically is selected. If not selected, click in the radio button to the left of it to select it. This setting is required to enable the DHCP server to automatically assign an IP address.
- Click **OK** to continue.

Restart the PC.

Repeat these steps for each PC with this version of Windows on your network.


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel

Selecting Windows' Internet Access Method

1. On the Windows taskbar, click the **Start** button, point to **Settings**, and then click **Control Panel**.
2. Double-click the **Internet Options** icon.
3. Select **I want to set up my Internet connection manually** or **I want to connect through a Local Area Network** and click **Next**.
4. Select **I want to connect through a Local Area Network** and click **Next**.
5. Uncheck all boxes in the LAN Internet Configuration screen and click **Next**.
6. Proceed to the end of the Wizard.

Verifying TCP/IP Properties

After your PC is configured and has rebooted, you can check the TCP/IP configuration using the utility *winipcfg.exe*:

1. On the Windows taskbar, click the **Start** button, and then click **Run**.
2. Type **winipcfg**, and then click **OK**.

   The IP Configuration window opens, which lists (among other things), your IP address, subnet mask, and default gateway.
3. From the drop-down box, select your Ethernet adapter.

   The window is updated to show your settings, which should match the values below if you are using the default TCP/IP settings that NETGEAR recommends for connecting through a router or gateway:

   - The IP address is between 192.168.0.2 and 192.168.0.254
   - The subnet mask is 255.255.255.0
   - The default gateway is 192.168.0.1

Configuring Windows NT4, 2000 or XP for IP Networking

As part of the PC preparation process, you may need to install and configure TCP/IP on each networked PC. Before starting, locate your Windows CD; you may need to insert it during the TCP/IP installation process.

Install or Verify Windows Networking Components

To install or verify the necessary components for IP networking:

1. On the Windows taskbar, click the **Start** button, point to **Settings**, and then click **Control Panel**.
2. Double-click the **Network and Dialup Connections** icon.
3. If an Ethernet adapter is present in your PC, you should see an entry for **Local Area Connection**. Double-click that entry.
4. Select **Properties**.
5. Verify that **Client for Microsoft Networks** and **Internet Protocol (TCP/IP)** are present. If not, select **Install** and add them.
6. Select **Internet Protocol (TCP/IP)**, click **Properties**, and verify that **Obtain an IP address automatically** is selected.
7. Click **OK** and close all **Network and Dialup Connections** windows.

8. Then, restart your PC.

Enabling DHCP to Automatically Configure TCP/IP Settings

You will find there are many similarities in the procedures for different Windows systems when using DHCP to configure TCP/IP.

The following steps will walk you through the configuration process for each of these versions of Windows.

DHCP Configuration of TCP/IP in Windows XP

1

Locate your **Network Neighborhood** icon.

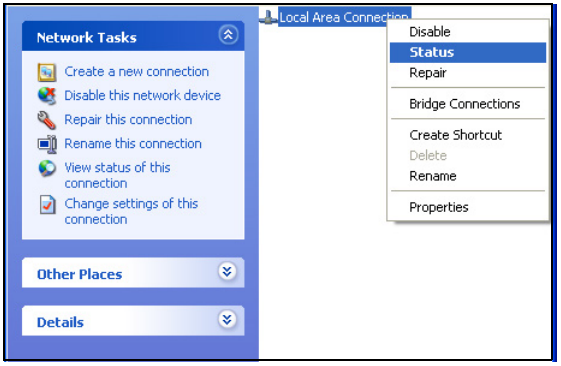
- Select **Control Panel** from the Windows XP new Start Menu.
- Select the **Network Connections** icon on the Control Panel. This will take you to the next step.

2

- Now the Network Connection window displays.

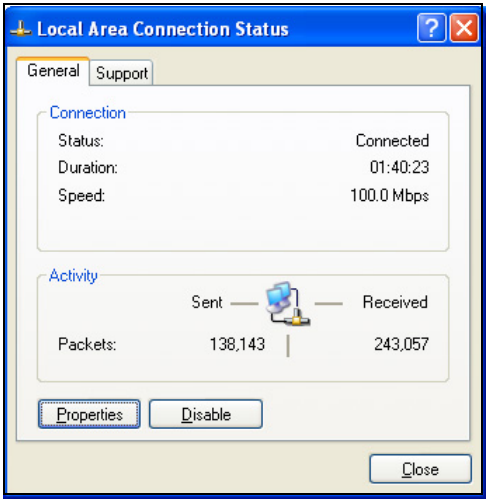
  The Connections List that shows all the network connections set up on the PC, located to the right of the window.

- Right-click on the **Connection** you will use and choose **Status**.



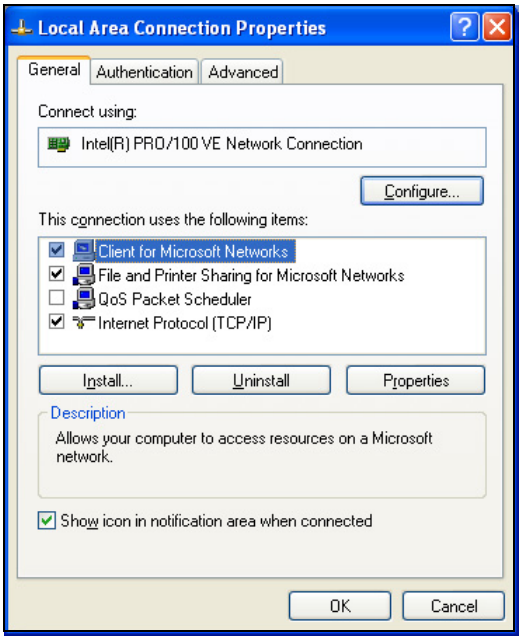
3

- Now you should be at the Local Area Network Connection Status window. This box displays the connection status, duration, speed, and activity statistics.
- Administrator logon access rights are needed to use this window.
- Click the **Properties button** to view details about the connection.



4

- The TCP/IP details are presented on the Support tab page.
- Select **Internet Protocol,** and click **Properties** to view the configuration information**.**

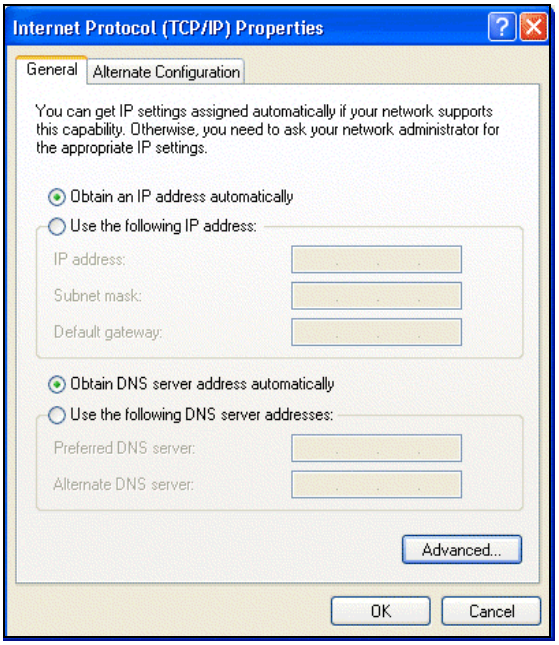


5

- Verify that the **Obtain an IP address automatically** radio button is selected.
- Verify that **Obtain DNS server address automatically** radio button is selected.
- Click the **OK** button.

This completes the DHCP configuration of TCP/IP in Windows XP.

Repeat these steps for each PC with this version of Windows on your network.


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

DHCP Configuration of TCP/IP in Windows 2000

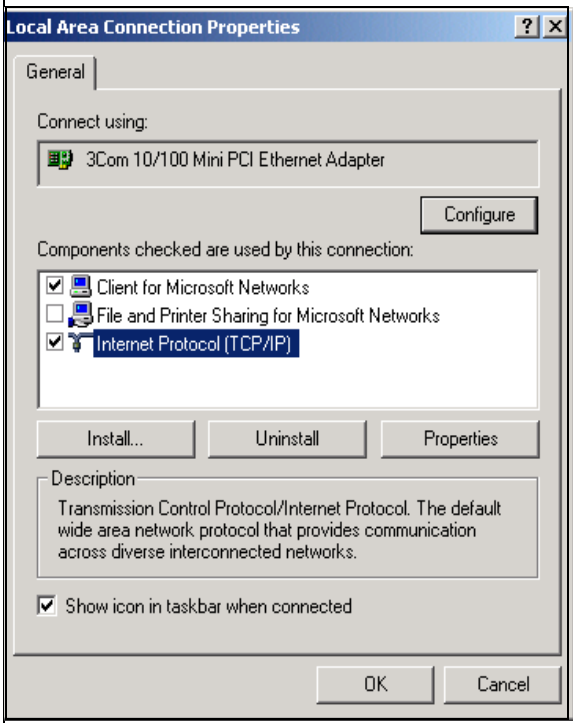
Once again, after you have installed the network card, TCP/IP for Windows 2000 is configured. TCP/IP should be added by default and set to DHCP without your having to configure it. However, if there are problems, follow these steps to configure TCP/IP with DHCP for Windows 2000.

1

- Click on the **My Network Places** icon on the Windows desktop. This will bring up a window called Network and Dial-up Connections.
- Right click on **Local Area Connection** and select **Properties**.

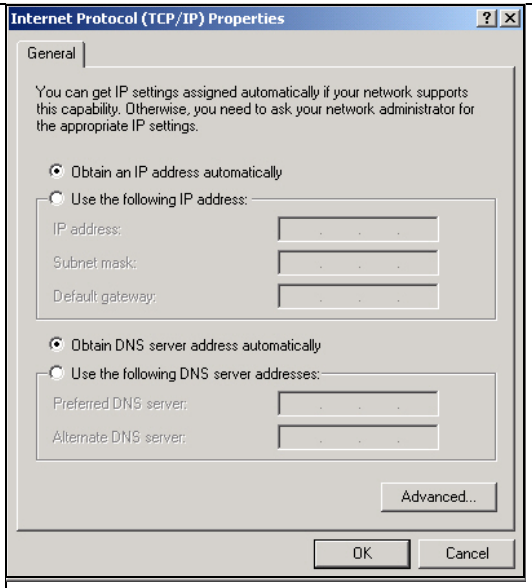
2

- The **Local Area Connection Properties** dialog box appears.
- Verify that you have the correct Ethernet card selected in the **Connect using:** box.
- Verify that at least the following two items are displayed and selected in the box of "Components checked are used by this connection:"
  - Client for Microsoft Networks and
  - Internet Protocol (TCP/IP)
- Click **OK**.



3

- With Internet Protocol (TCP/IP) selected, click on **Properties** to open the Internet Protocol (TCP/IP) Properties dialogue box.
- Verify that
  - **Obtain an IP address automatically** is selected.
  - **Obtain DNS server address automatically** is selected.
- Click **OK** to return to Local Area Connection Properties.

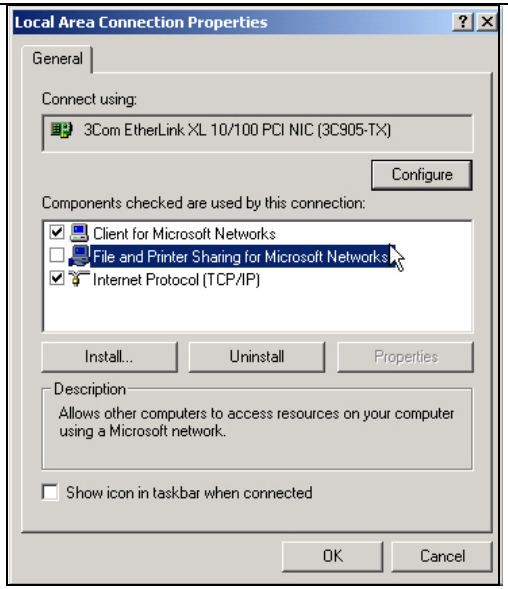

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

4

- Click **OK** again to complete the configuration process for Windows 2000.

Restart the PC.

Repeat these steps for each PC with this version of Windows on your network.



DHCP Configuration of TCP/IP in Windows NT4

Once you have installed the network card, you need to configure the TCP/IP environment for Windows NT 4.0. Follow this procedure to configure TCP/IP with DHCP in Windows NT 4.0.

1

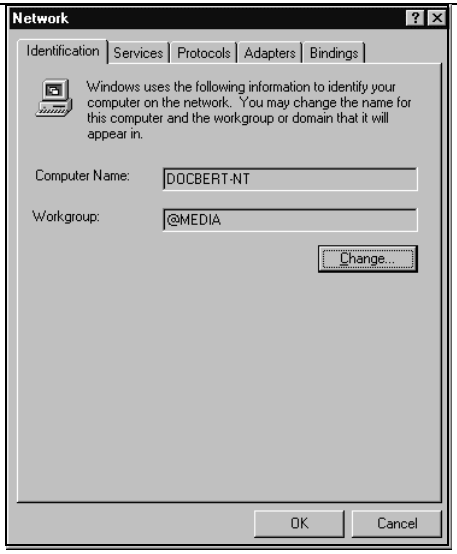
- Choose **Settings** from the Start Menu, and then select **Control Panel**. This will display Control Panel window.

2

- Double-click the **Network** icon in the Control Panel window.

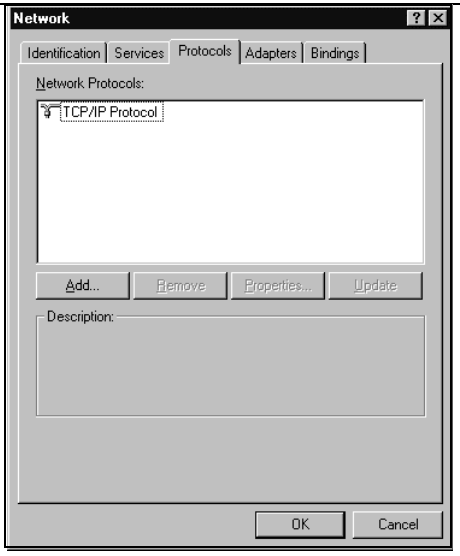
  The Network panel will display.

- Select the **Protocols** tab to continue.



3

- Highlight the **TCP/IP Protocol** in the **Network Protocols** box, and click on the **Properties** button.

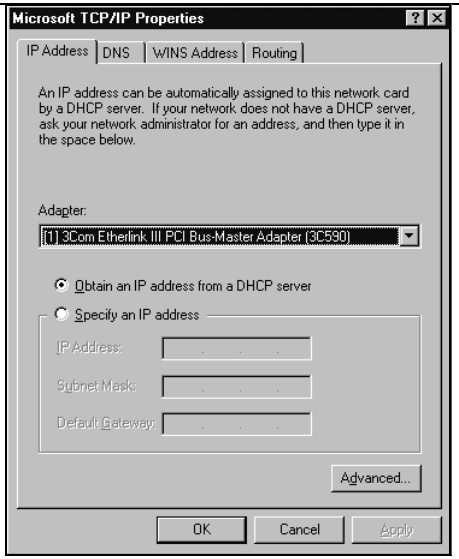


4

- The **TCP/IP Properties** dialog box now displays.
- Click the **IP Address** tab**.**
- Select the radio button marked **Obtain an IP address from a DHCP server.**
- Click **OK**. This completes the configuration of TCP/IP in Windows NT.

Restart the PC.

Repeat these steps for each PC with this version of Windows on your network.


Microsoft TCP/IP Properties
IP Address
DNS
WINS Address
Routing
An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.
Adapter:
[1] 3Com Etherlink III PCI Bus-Master Adapter (3C590)
Obtain an IP address from a DHCP server
Specify an IP address
IP Address:
Subnet Mask:
Default Gateway:
Advanced...
OK
Cancel
Apply

Verifying TCP/IP Properties for Windows XP, 2000, and NT4

To check your PC's TCP/IP configuration:

1. On the Windows taskbar, click the **Start** button, and then click **Run**.

   The Run window opens.

2. Type **`cmd`** and then click **OK**.

   A command window opens

3. Type **`ipconfig /all`**

   Your IP Configuration information will be listed, and should match the values below if you are using the default TCP/IP settings that NETGEAR recommends for connecting through a router or gateway:

   - The IP address is between 192.168.0.2 and 192.168.0.254
   - The subnet mask is 255.255.255.0

- The default gateway is 192.168.0.1

4. Type **exit**

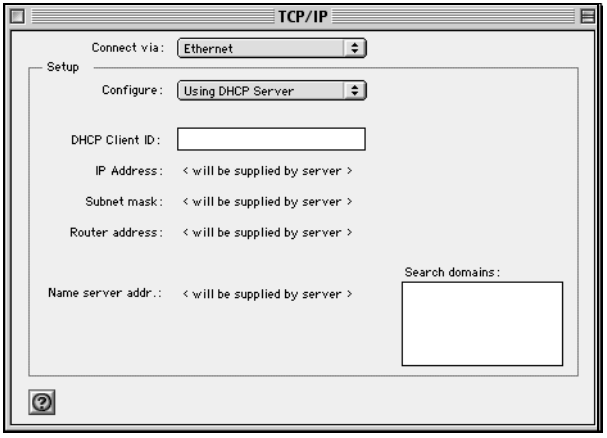
Configuring the Macintosh for TCP/IP Networking

Beginning with Macintosh Operating System 7, TCP/IP is already installed on the Macintosh. On each networked Macintosh, you will need to configure TCP/IP to use DHCP.

MacOS 8.6 or 9.x

1. From the Apple menu, select Control Panels, then TCP/IP.

   The TCP/IP Control Panel opens:



2. From the “Connect via” box, select your Macintosh’s Ethernet interface.
3. From the “Configure” box, select Using DHCP Server.

   You can leave the DHCP Client ID box empty.

4. Close the TCP/IP Control Panel.
5. Repeat this for each Macintosh on your network.

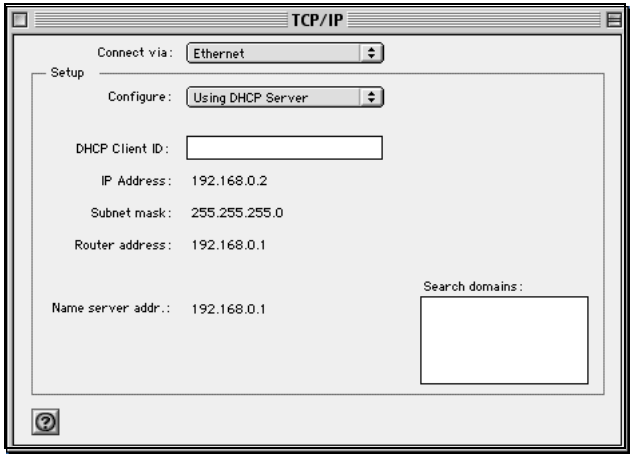
MacOS X

1. From the Apple menu, choose System Preferences, then Network.

2. If not already selected, select Built-in Ethernet in the Configure list.
3. If not already selected, Select Using DHCP in the TCP/IP tab.
4. Click **Save**.

Verifying TCP/IP Properties for Macintosh Computers

After your Macintosh is configured and has rebooted, you can check the TCP/IP configuration by returning to the TCP/IP Control Panel. From the Apple menu, select Control Panels, then TCP/IP.



The panel is updated to show your settings, which should match the values below if you are using the default TCP/IP settings that NETGEAR recommends:

- The IP Address is between 192.168.0.2 and 192.168.0.254
- The Subnet mask is 255.255.255.0
- The Router address is 192.168.0.1

If you do not see these values, you may need to restart your Macintosh or you may need to switch the “Configure” setting to a different option, then back again to “Using DHCP Server”.

Verifying the Readiness of Your Internet Account

For broadband access to the Internet, you need to contract with an Internet service provider (ISP) for a single-user Internet access account using a cable modem or DSL modem. This modem must be a separate physical box (not a card) and must provide an Ethernet port intended for connection to a Network Interface Card (NIC) in a computer. Your firewall does not support a USB-connected broadband modem.

For a single-user Internet account, your ISP supplies TCP/IP configuration information for one computer. With a typical account, much of the configuration information is dynamically assigned when your PC is first booted up while connected to the ISP, and you will not need to know that dynamic information.

In order to share the Internet connection among several computers, your firewall takes the place of the single PC, and you need to configure it with the TCP/IP information that the single PC would normally use. When the firewall's Internet port is connected to the broadband modem, the firewall appears to be a single PC to the ISP. The firewall then allows the PCs on the local network to masquerade as the single PC to access the Internet through the broadband modem. The method used by the firewall to accomplish this is called Network Address Translation (NAT) or IP masquerading.

Are Login Protocols Used?

Some ISPs require a special login protocol, in which you must enter a login name and password in order to access the Internet. If you normally log in to your Internet account by running a program such as WinPOET or EnterNet, then your account uses PPP over Ethernet (PPPoE).

When you configure your router, you will need to enter your login name and password in the router's configuration menus. After your network and firewall are configured, the firewall will perform the login task when needed, and you will no longer need to run the login program from your PC. It is not necessary to uninstall the login program.

What Is Your Configuration Information?

More and more, ISPs are dynamically assigning configuration information. However, if your ISP does not dynamically assign configuration information but instead used fixed configurations, your ISP should have given you the following basic information for your account:

- An IP address and subnet mask
- A gateway IP address, which is the address of the ISP's router
- One or more domain name server (DNS) IP addresses
- Host name and domain suffix

  For example, your account's full server names may look like this:

  `mail.xxx.yyy.com`

  In this example, the domain suffix is `xxx.yyy.com`.

If any of these items are dynamically supplied by the ISP, your firewall automatically acquires them.

If an ISP technician configured your PC during the installation of the broadband modem, or if you configured it using instructions provided by your ISP, you need to copy the configuration information from your PC's Network TCP/IP Properties window or Macintosh TCP/IP Control Panel before reconfiguring your PC for use with the firewall. These procedures are described next.

Obtaining ISP Configuration Information for Windows Computers

As mentioned above, you may need to collect configuration information from your PC so that you can use this information when you configure the FVS318v3 VPN Firewall. Following this procedure is only necessary when your ISP does not dynamically supply the account information.

To get the information you need to configure the firewall for Internet access:

1. On the Windows taskbar, click the **Start** button, point to **Settings**, and then click **Control Panel**.
2. Double-click the **Network** icon.

   The Network window opens, which displays a list of installed components.
3. Select **TCP/IP**, and then click **Properties**.

   The TCP/IP Properties dialog box opens.
4. Select the **IP Address** tab.

   If an IP address and subnet mask are shown, write down the information. If an address is present, your account uses a fixed (static) IP address. If no address is present, your account uses a dynamically-assigned IP address. Click "Obtain an IP address automatically".
5. Select the **Gateway** tab.

If an IP address appears under Installed Gateways, write down the address. This is the ISP's gateway address. Select the address and then click **Remove** to remove the gateway address.

6. Select the DNS Configuration tab.

   If any DNS server addresses are shown, write down the addresses. If any information appears in the Host or Domain information box, write it down. Click **Disable DNS**.

7. Click **OK** to save your changes and close the TCP/IP Properties dialog box.

   You are returned to the Network window.

8. Click **OK**.

9. Reboot your PC at the prompt. You may also be prompted to insert your Windows CD.

Obtaining ISP Configuration Information for Macintosh Computers

As mentioned above, you may need to collect configuration information from your Macintosh so that you can use this information when you configure the FVS318v3 VPN Firewall. Following this procedure is only necessary when your ISP does not dynamically supply the account information.

To get the information you need to configure the firewall for Internet access:

1. From the Apple menu, select Control Panels, then TCP/IP.

   The TCP/IP Control Panel opens, which displays a list of configuration settings. If the "Configure" setting is "Using DHCP Server", your account uses a dynamically-assigned IP address. In this case, close the Control Panel and skip the rest of this section.

2. If an IP address and subnet mask are shown, write down the information.

3. If an IP address appears under Router address, write down the address. This is the ISP's gateway address.

4. If any Name Server addresses are shown, write down the addresses. These are your ISP's DNS addresses.

5. If any information appears in the Search domains information box, write it down.

6. Change the "Configure" setting to "Using DHCP Server".

7. Close the TCP/IP Control Panel.

Restarting the Network

Once you've set up your computers to work with the firewall, you must reset the network for the devices to be able to communicate correctly. Restart any computer that is connected to the FVS318v3 VPN Firewall.

After configuring all of your computers for TCP/IP networking and restarting them, and connecting them to the local network of your FVS318v3 VPN Firewall, you are ready to access and configure the firewall.

Appendix E
VPN Configuration of NETGEAR FVS318v3

This is a case study on how to configure a secure IPSec VPN tunnel on a NETGEAR FVS318v3. This case study follows the VPN Consortium interoperability profile guidelines (found at *http://www.vpnc.org/InteropProfiles/Interop-01.html*).

This study covers the following situations:

- FVS318v3 to FVS318v3 (see page E-6)
- FVS318v3 to FVS318v2 (see page E-13)
- FVS318v3 to FVL328 (see page E-20)
- FVS318v3 to VPN Client (see page E-27)

Note: Product updates are available on the NETGEAR, Inc. Web site at *http://www.netgear.com/support/main.asp*.

Case Study Overview

The procedure for configuring a VPN tunnel between two gateway endpoints is as follows:

1. **Gather the network information**
2. **Configure gateway A**
3. **Configure gateway B**
4. **Activate the VPN tunnel**

Gathering the Network Information

The configuration in this document follows the addressing and configuration mechanics defined by the VPN Consortium. Gather all the necessary information before you begin the configuration process. Verify whether the firmware is up to date, all of the addresses that will be necessary, and all of the parameters that need to be set on both sides. Check that there are no firewall restrictions.

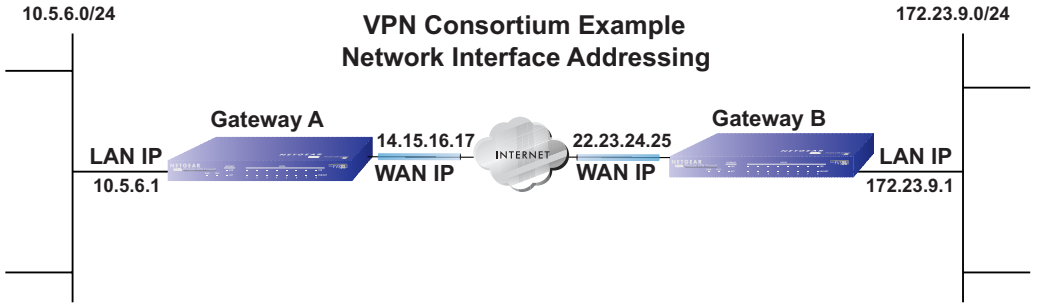


Figure E-1: Addressing and subnets used for this case study

Configuring the Gateways

Configure each gateway as summarized in Figure E-2 and Figure E-3:

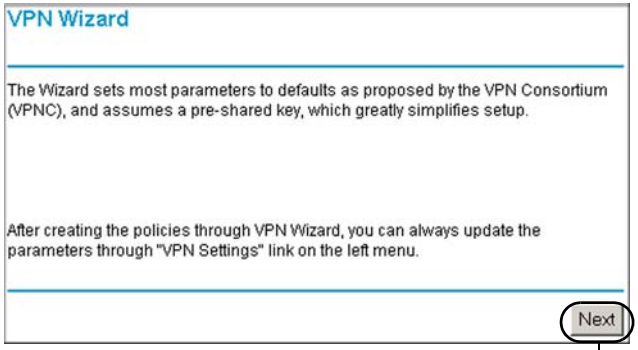
1. **Configure Gate A.**
   a. **Log in to the router at Gateway A.**
   b. **Use the VPN Wizard to configure this router.**

      Enter the requested information as prompted by the VPN Wizard:

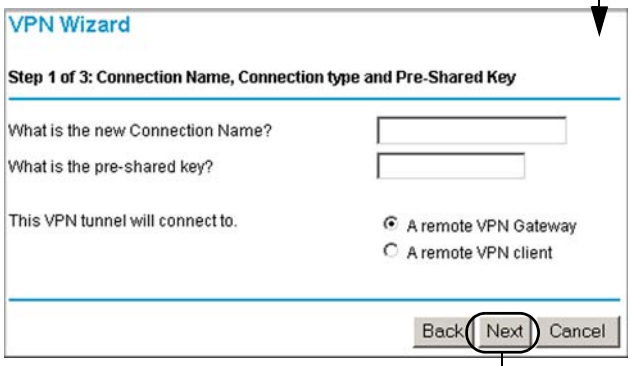
      - Connection Name and Pre-Shared Key
      - Remote WAN IP address
      - Remote LAN IP Subnet: IP Address and Subnet Mask:
2. **Repeat the above steps for Gateway B.**
   a. **Log in to the router at Gateway B.**
   b. **Use the VPN Wizard to configure this router.**

      Enter the requested information as prompted by the VPN Wizard.

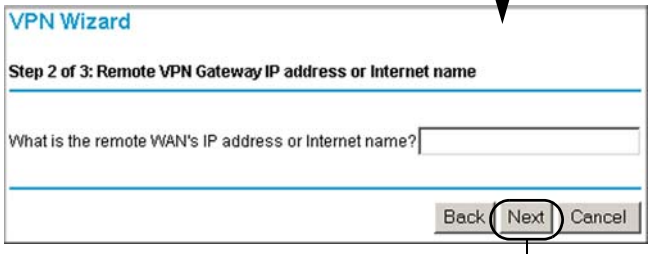
	Note: The WAN and LAN IP addresses must be unique at each end of the VPN tunnel.


VPN Wizard
The Wizard sets most parameters to defaults as proposed by the VPN Consortium (VPNC), and assumes a pre-shared key, which greatly simplifies setup.
After creating the policies through VPN Wizard, you can always update the parameters through "VPN Settings" link on the left menu.
Next

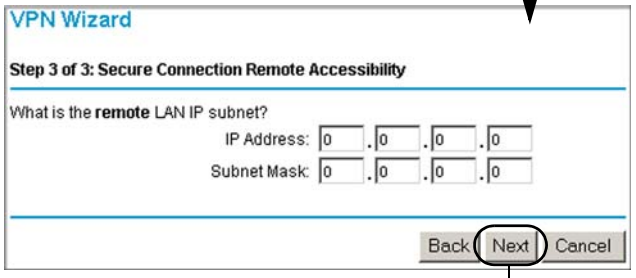
Step 1: Click VPN Wizard on the Side Menu Bar


VPN Wizard
Step 1 of 3: Connection Name, Connection type and Pre-Shared Key
What is the new Connection Name?
What is the pre-shared key?
This VPN tunnel will connect to.
A remote VPN Gateway
A remote VPN client
Back
Next
Cancel

Step 2: Enter the following:
- **Connection name**
- **Pre-Shared Key (must be the same for each end)**
- **Select "A remote VPN Gateway"**


VPN Wizard
Step 2 of 3: Remote VPN Gateway IP address or Internet name
What is the remote WAN's IP address or Internet name?
Back
Next
Cancel

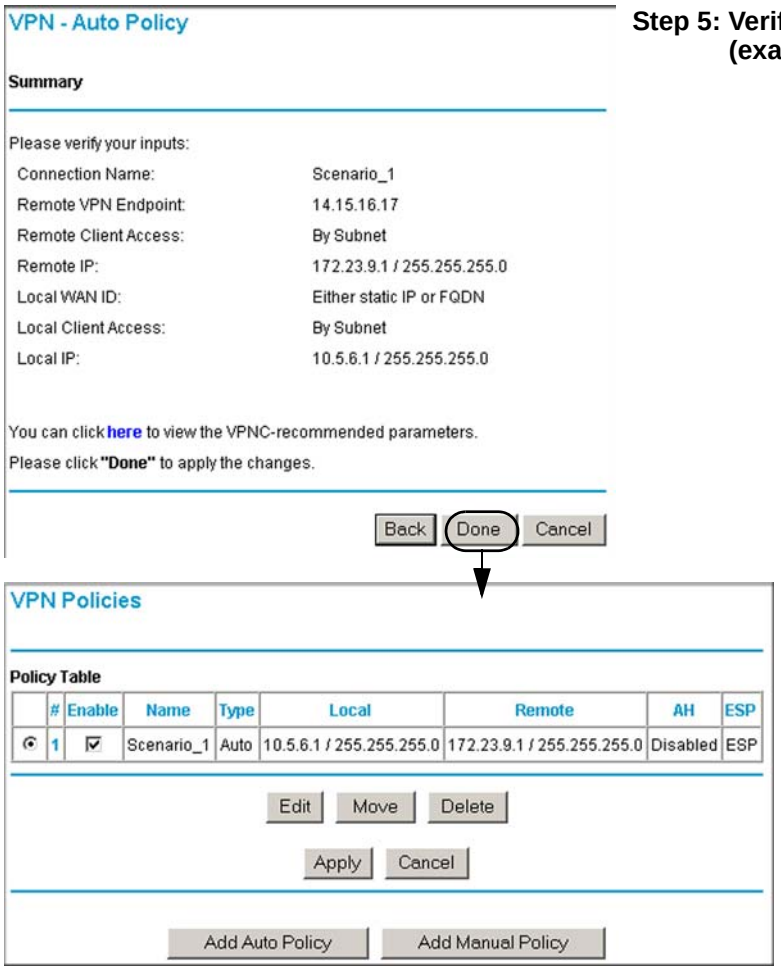
Step 3: Enter the remote WAN's IP address


VPN Wizard
Step 3 of 3: Secure Connection Remote Accessibility
What is the remote LAN IP subnet?
IP Address: 0 . 0 . 0 . 0
Subnet Mask: 0 . 0 . 0 . 0
Back
Next
Cancel

Step 4: Enter the following:
- **Remote LAN IP Address**
- **Remote LAN Subnet Mask**

to Figure E-3

Figure E-2: NETGEAR's VPN Wizard for the router at each gateway (part 1 of 2)



Step 5: Verify the information (example screen)

Example screen

Figure E-3: NETGEAR's VPN Wizard for the router at a gateway A (part 2 of 2)

Note: The default log in address for the FVS318v3 router is *http://192.168.0.1* with the default user name of **admin** and default password of **password**. The login address will change to the local LAN IP subnet address after you configure the router. The user name and password will also change to the ones you have chosen to use in your installation.

Activating the VPN Tunnel

You can activate the VPN tunnel by testing connectivity and viewing the VPN tunnel status information as described in the following flowchart:

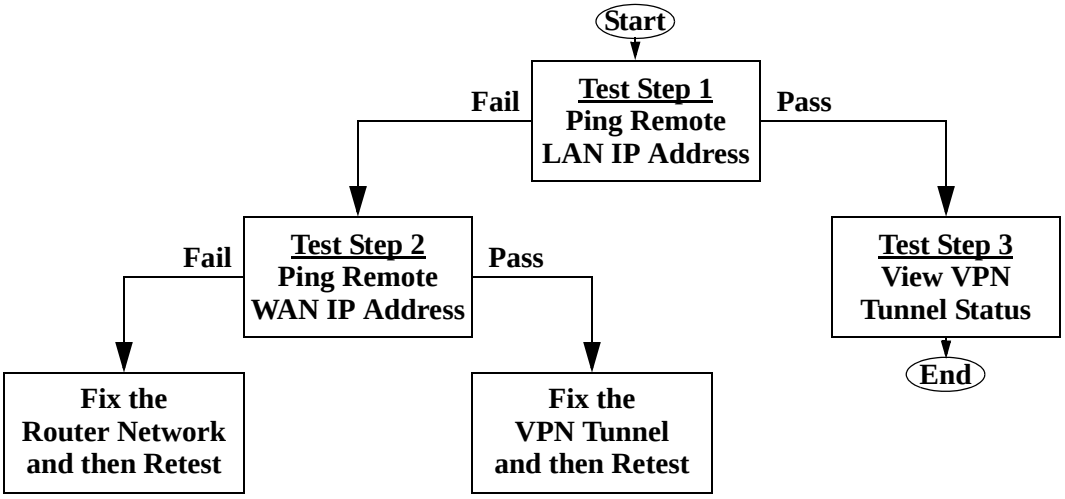


Figure E-4: Testing Flowchart

All traffic from the range of LAN IP addresses specified on the router at Gateway A and the router at Gateway B will now flow over a secure VPN tunnel.

The FVS318v3-to-FVS318v3 Case

Table E-1. Policy Summary

VPN Consortium Scenario:		Scenario 1
Type of VPN		LAN-to-LAN or Gateway-to-Gateway
Security Scheme:		IKE with Preshared Secret/Key
Date Tested:		November 2004
Model/Firmware Tested:		
	NETGEAR-Gateway A	FVS318v3 with firmware version v3.0_14
	NETGEAR-Gateway B	FVS318v3 with firmware version v3.0_14
IP Addressing:		
	NETGEAR-Gateway A	Static IP address
	NETGEAR-Gateway B	Static IP address

Configuring the VPN Tunnel

Note: This scenario assumes all ports are open on the FVS318v3.

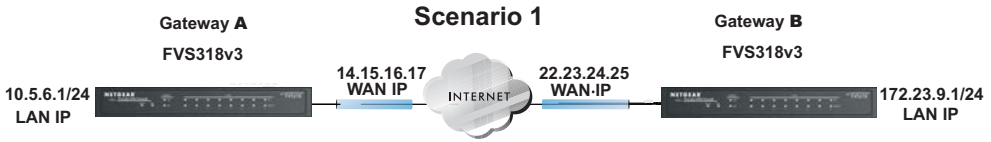


Figure E-5: LAN to LAN VPN access from an FVS318v3 to an FVS318v3

Use this scenario illustration and configuration screens as a model to build your configuration.

1. **Log in to the FVS318v3 labeled Gateway A as in the illustration (Figure E-5).**

   Log in at the default address of *http://192.168.0.1* with the default user name of **admin** and default password of **password** (or using whatever password and LAN address you have chosen).

Note: Based on the network addresses used in this example, you would log in to the LAN IP address of *http://10.5.6.1* at Gateway A.

2. Use the VPN Wizard to configure the FVS318v3 at Gateway A.

Follow the steps listed in Figure E-2 and Figure E-3 using the following parameters as illustrated in Figure E-6:

- Connection Name: **Scenario_1** (in this example)
- Pre-Shared Key: **12345678** (in this example), must be the same at both VPN tunnel endpoints
- Remote WAN IP address: **22.23.24.25** (in this example), must be unique at each VPN tunnel endpoint
- Remote LAN IP Subnet
  - IP Address: **172.23.9.1** (in this example), must be unique at each VPN tunnel endpoint
  - Subnet Mask: **255.255.255.0** (in this example)

3. **Log in to the FVS318v3 labeled Gateway B as in the illustration (Figure E-5).**

Log in at the default address of *http://192.168.0.1* with the default user name of **admin** and default password of **password** (or using whatever password and LAN address you have chosen).

Note: Based on the network addresses used in this example, you would log in to the LAN IP address of *http://172.23.9.1* at Gateway B.

4. Repeat the process using the VPN Wizard to configure the FVS318v3 at Gateway B.

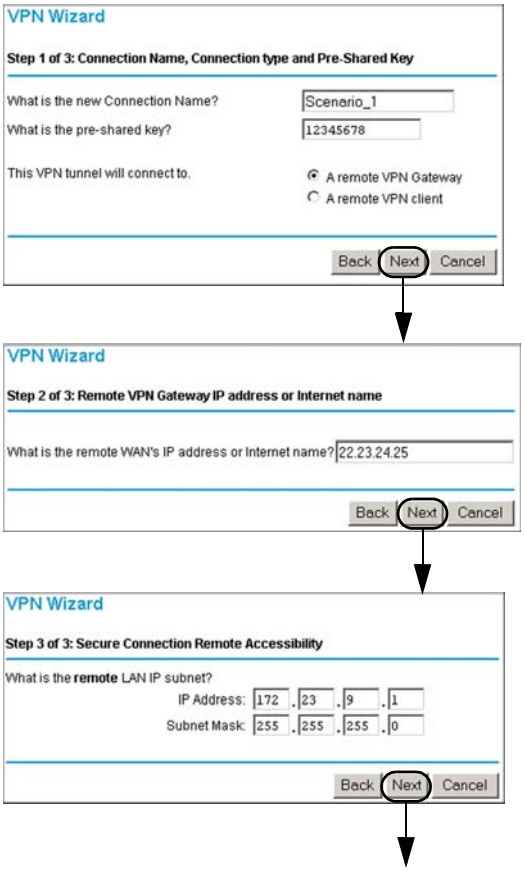
Follow the steps listed in Figure E-2 and Figure E-3, but use the following parameters instead as illustrated in Figure E-6:

- Connection Name: **Scenario_1** (in this example)
- Pre-Shared Key: **12345678** (in this example), must be the same at both VPN tunnel endpoints
- Remote WAN IP address: **14.15.16.17** (in this example), must be unique at each VPN tunnel endpoint

- Remote LAN IP Subnet
  - IP Address: **10.5.6.1** (in this example), must be unique at each VPN tunnel endpoint
  - Subnet Mask: **255.255.255.0** (in this example)

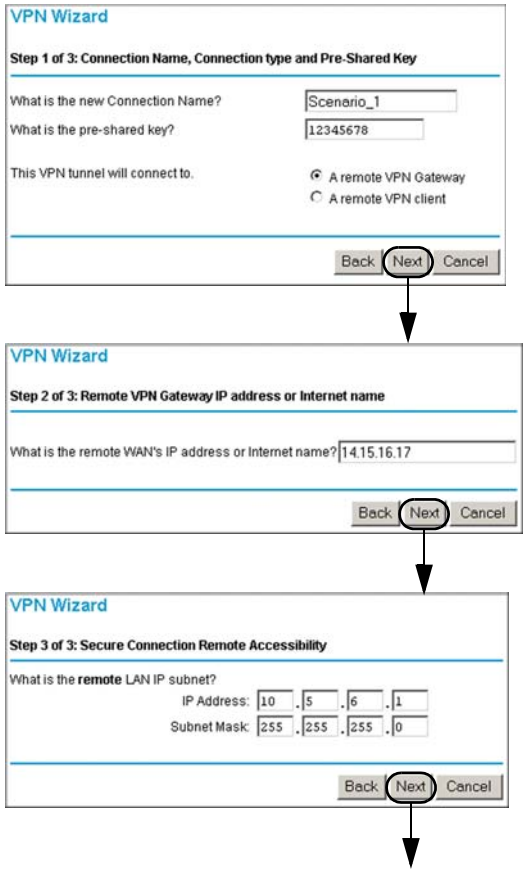
All traffic from the range of LAN IP addresses specified on FVS318v3 A and FVS318v3 B will now flow over a secure VPN tunnel once the VPN tunnel is initiated (see "Initiating and Checking the VPN Connections" on page 11).

Gateway A VPN Parameter Entry


VPN Wizard
Step 1 of 3: Connection Name, Connection type and Pre-Shared Key
What is the new Connection Name?
Scenario_1
What is the pre-shared key?
12345678
This VPN tunnel will connect to.
A remote VPN Gateway
A remote VPN client
Back
Next
Cancel
VPN Wizard
Step 2 of 3: Remote VPN Gateway IP address or Internet name
What is the remote WAN's IP address or Internet name?
22.23.24.25
Back
Next
Cancel
VPN Wizard
Step 3 of 3: Secure Connection Remote Accessibility
What is the remote LAN IP subnet?
IP Address: 172 . 23 . 9 . 1
Subnet Mask: 255 . 255 . 255 . 0
Back
Next
Cancel

Continue as shown in Figure E-3

Gateway B VPN Parameter Entry


VPN Wizard
Step 1 of 3: Connection Name, Connection type and Pre-Shared Key
What is the new Connection Name?
Scenario_1
What is the pre-shared key?
12345678
This VPN tunnel will connect to.
A remote VPN Gateway
A remote VPN client
Back
Next
Cancel
VPN Wizard
Step 2 of 3: Remote VPN Gateway IP address or Internet name
What is the remote WAN's IP address or Internet name?
14.15.16.17
Back
Next
Cancel
VPN Wizard
Step 3 of 3: Secure Connection Remote Accessibility
What is the remote LAN IP subnet?
IP Address: 10 . 5 . 6 . 1
Subnet Mask: 255 . 255 . 255 . 0
Back
Next
Cancel

Continue as shown in Figure E-3

Figure E-6: VPN parameter entry at Gateway A (FVS318v3) and Gateway B (FVS318v3)

Viewing and Editing the VPN Parameters

The VPN Wizard sets up a VPN tunnel using the default parameters from the VPN Consortium (VPNC). The policy definitions to manage VPN traffic on the FVS318v3 are presented in Figure E-7 and Figure E-8.

Gateway A VPN Policy Parameters **Gateway B VPN Policy Parameters**

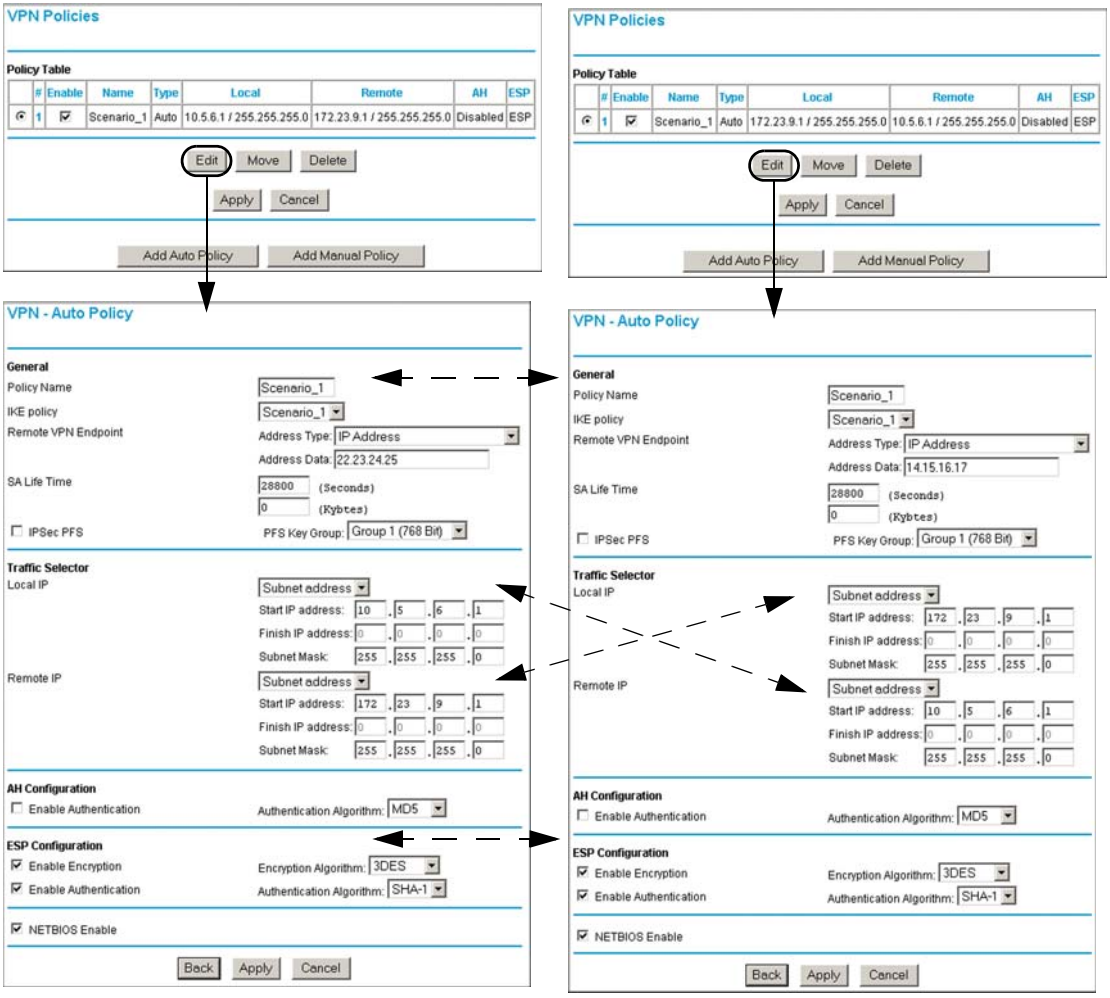

VPN Policies
Policy Table
Enable Name Type Local Remote AH ESP
1 Scenario_1 Auto 10.5.6.1 / 255.255.255.0 172.23.9.1 / 255.255.255.0 Disabled ESP
Edit Move Delete
Apply Cancel
Add Auto Policy Add Manual Policy
VPN - Auto Policy
General
Policy Name Scenario_1
IKE policy Scenario_1
Remote VPN Endpoint Address Type: IP Address
Address Data: 22.23.24.25
SA Life Time 28800 (Seconds) 0 (Kybtes)
IPSec PFS PFS Key Group: Group 1 (768 Bit)
Traffic Selector
Local IP Subnet address
Start IP address: 10.5.6.1
Finish IP address: 0.0.0.0
Subnet Mask: 255.255.255.0
Remote IP Subnet address
Start IP address: 172.23.9.1
Finish IP address: 0.0.0.0
Subnet Mask: 255.255.255.0
AH Configuration
Enable Authentication Authentication Algorithm: MD5
ESP Configuration
Enable Encryption Encryption Algorithm: 3DES
Enable Authentication Authentication Algorithm: SHA-1
NETBIOS Enable
Back Apply Cancel
VPN Policies
Policy Table
Enable Name Type Local Remote AH ESP
1 Scenario_1 Auto 172.23.9.1 / 255.255.255.0 10.5.6.1 / 255.255.255.0 Disabled ESP
Edit Move Delete
Apply Cancel
Add Auto Policy Add Manual Policy
VPN - Auto Policy
General
Policy Name Scenario_1
IKE policy Scenario_1
Remote VPN Endpoint Address Type: IP Address
Address Data: 14.15.16.17
SA Life Time 28800 (Seconds) 0 (Kybtes)
IPSec PFS PFS Key Group: Group 1 (768 Bit)
Traffic Selector
Local IP Subnet address
Start IP address: 172.23.9.1
Finish IP address: 0.0.0.0
Subnet Mask: 255.255.255.0
Remote IP Subnet address
Start IP address: 10.5.6.1
Finish IP address: 0.0.0.0
Subnet Mask: 255.255.255.0
AH Configuration
Enable Authentication Authentication Algorithm: MD5
ESP Configuration
Enable Encryption Encryption Algorithm: 3DES
Enable Authentication Authentication Algorithm: SHA-1
NETBIOS Enable
Back Apply Cancel

Figure E-7: VPN policies at Gateway A (FVS318v3) and Gateway B (FVS318v3)

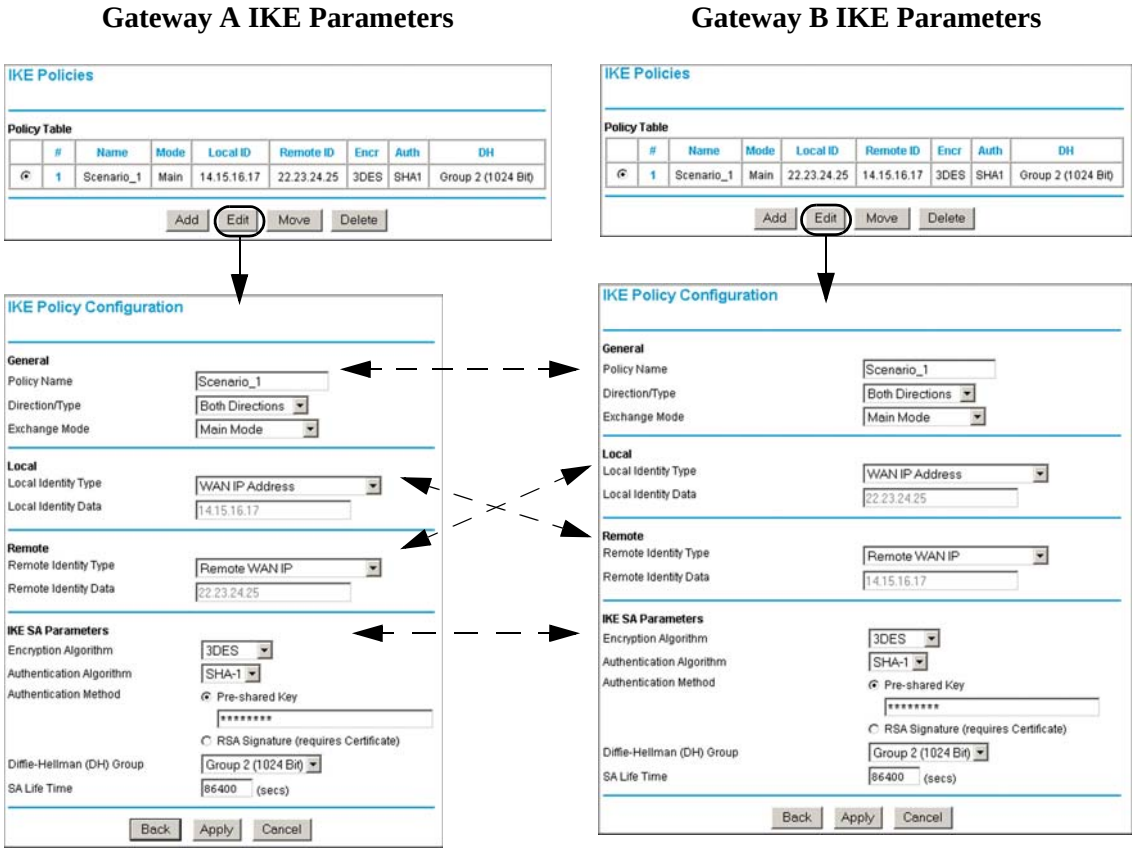


Figure E-8: IKE parameters at Gateway A (FVS318v3) and Gateway B (FVS318v3)

Note: The Pre-Shared Key must be the same at both VPN tunnel endpoints.

The remote WAN and LAN IP addresses for one VPN tunnel endpoint will be the local WAN and LAN IP addresses for the other VPN tunnel endpoint.

The VPN Wizard ensures the other VPN parameters are the same at both VPN tunnel endpoints.

Initiating and Checking the VPN Connections

You can test connectivity and view VPN status information on the FVS318v3 according to the testing flowchart shown in Figure E-4. To test the VPN tunnel from the Gateway A LAN, do the following:

1. **Test 1: Ping Remote LAN IP Address**: To establish the connection between the FVS318v3 Gateway A and Gateway B tunnel endpoints, perform these steps at Gateway A:

   a. From a Windows PC attached to the FVS318v3 on LAN A, click the **Start** button on the taskbar and then click **Run**.

   b. Type **ping -t 172.23.9.1**, and then click **OK** (you would type **ping -t 10.5.6.1** if testing from Gateway B).

   c. This will cause a continuous ping to be sent to the LAN interface of Gateway B. Within two minutes, the ping response should change from timed out to reply.

   At this point the VPN-tunnel-endpoint-to-VPN-tunnel-endpoint connection is established.

2. **Test 2: Ping Remote WAN IP Address (if Test 1 fails)**: To test connectivity between the Gateway A and Gateway B WAN ports, follow these steps:

   a. Log in to the router on LAN A, go to the main menu Maintenance section, and click the **Diagnostics** link.

   b. To test connectivity to the WAN port of Gateway B, enter **22.23.24.25**, and then click **Ping** (you would enter **14.15.16.17** if testing from Gateway B).

   c. This causes a ping to be sent to the WAN interface of Gateway B. Within two minutes, the ping response should change from timed out to reply. You may have to run this test several times before you get the reply message back from the target FVS318v3.

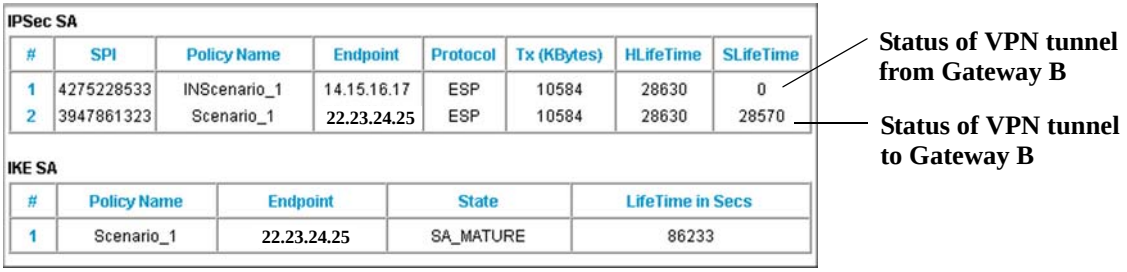
   d. At this point the gateway-to-gateway connection is verified.

3. **Test 3: View VPN Tunnel Status**: To view the FVS318v3 event log and status of Security Associations, follow these steps:

   a. Go to the FVS318v3 main menu VPN section and click the **VPN Status** link.

   b. The log screen displays a history of the VPN connections, and the IPSec SA and IKE SA tables report the status and data transmission statistics of the VPN tunnels for each policy.

VPN Status at Gateway A (FVS318v3)



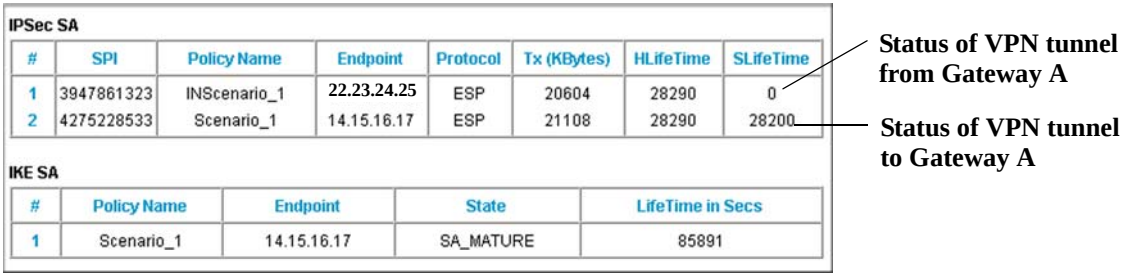
IPSec SA

#	SPI	Policy Name	Endpoint	Protocol	Tx (KBytes)	HLifeTime	SLifeTime
1	4275228533	INScenario_1	14.15.16.17	ESP	10584	28630	0
2	3947861323	Scenario_1	22.23.24.25	ESP	10584	28630	28570

IKE SA

#	Policy Name	Endpoint	State	LifeTime in Secs
1	Scenario_1	22.23.24.25	SA_MATURE	86233

VPN Status at Gateway B (FVS318v3)



IPSec SA

#	SPI	Policy Name	Endpoint	Protocol	Tx (KBytes)	HLifeTime	SLifeTime
1	3947861323	INScenario_1	22.23.24.25	ESP	20604	28290	0
2	4275228533	Scenario_1	14.15.16.17	ESP	21108	28290	28200

IKE SA

#	Policy Name	Endpoint	State	LifeTime in Secs
1	Scenario_1	14.15.16.17	SA_MATURE	85891

Figure E-9: VPN Status for the FVS318v3 routers at Gateway A and Gateway B

The FVS318v3-to-FVS318v2 Case

Table E-2. Policy Summary

VPN Consortium Scenario:		Scenario 1
Type of VPN		LAN-to-LAN or Gateway-to-Gateway
Security Scheme:		IKE with Preshared Secret/Key
Date Tested:		November 2004
Model/Firmware Tested:		
	NETGEAR-Gateway A	FVS318v3 with firmware version v3.0_14
	NETGEAR-Gateway B	FVS318v2 with firmware version V2.4
IP Addressing:		
	NETGEAR-Gateway A	Static IP address
	NETGEAR-Gateway B	Static IP address

Configuring the VPN Tunnel

Note: This scenario assumes all ports are open on the FVS318v3 and FVS318v2.

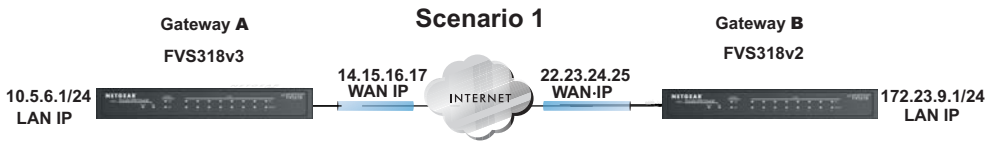


Figure E-10: LAN to LAN VPN access from an FVS318v3 to an FVS318v2

Use this scenario illustration and configuration screens as a model to build your configuration.

1. **Log in to the FVS318v3 labeled Gateway A as in the illustration (Figure E-10).**

   Log in at the default address of *http://192.168.0.1* with the default user name of **admin** and default password of **password** (or using whatever password and LAN address you have chosen).

Note: Based on the network addresses used in this example, you would log in to the LAN IP address of *http://10.5.6.1* at Gateway A.

2. Use the VPN Wizard to configure the FVS318v3 at Gateway A.

Follow the steps listed in Figure E-2 and Figure E-3 using the following parameters as illustrated in Figure E-11:

- Connection Name: **Scenario_1** (in this example)
- Pre-Shared Key: **12345678** (in this example), must be the same at both VPN tunnel endpoints
- Remote WAN IP address: **22.23.24.25** (in this example), must be unique at each VPN tunnel endpoint
- Remote LAN IP Subnet
  - IP Address: **172.23.9.1** (in this example), must be unique at each VPN tunnel endpoint
  - Subnet Mask: **255.255.255.0** (in this example)

3. **Log in to the FVS318v2 labeled Gateway B as in the illustration (Figure E-10).**

Log in at the default address of *http://192.168.0.1* with the default user name of **admin** and default password of **password** (or using whatever password and LAN address you have chosen).

Note: Based on the network addresses used in this example, you would log in to the LAN IP address of *http://172.23.9.1* at Gateway B.

4. Repeat the process using the VPN Wizard to configure the FVS318v2 at Gateway B.

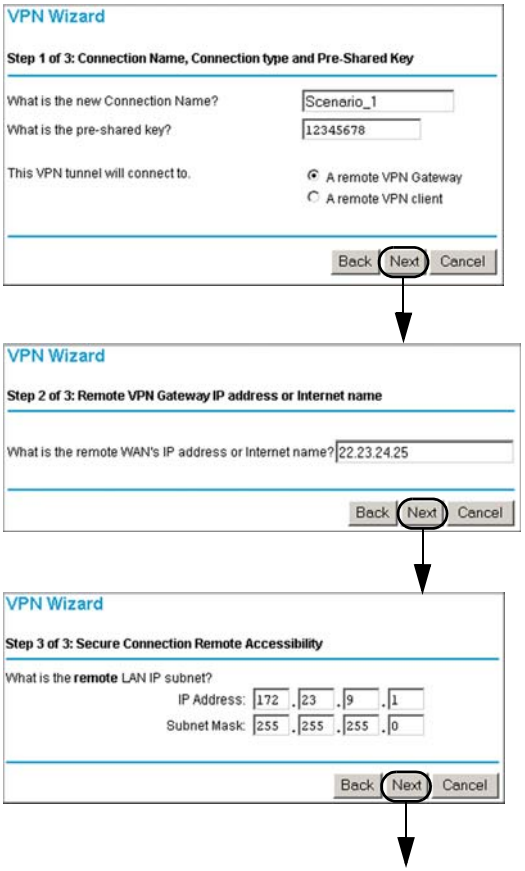
Follow the steps listed in Figure E-2 and Figure E-3, but use the following parameters instead as illustrated in Figure E-11:

- Connection Name: **Scenario_1** (in this example)
- Pre-Shared Key: **12345678** (in this example), must be the same at both VPN tunnel endpoints
- Remote WAN IP address: **14.15.16.17** (in this example), must be unique at each VPN tunnel endpoint

- Remote LAN IP Subnet
  - IP Address: **10.5.6.1** (in this example), must be unique at each VPN tunnel endpoint
  - Subnet Mask: **255.255.255.0** (in this example)

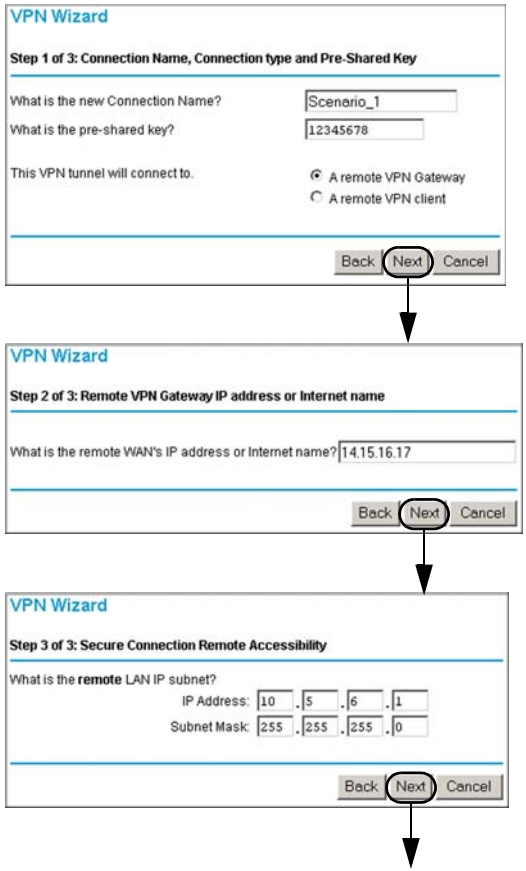
All traffic from the range of LAN IP addresses specified on FVS318v3 A and FVS318v3 B will now flow over a secure VPN tunnel once the VPN tunnel is initiated (see "Initiating and Checking the VPN Connections" on page 18).

Gateway A VPN Parameter Entry


VPN Wizard
Step 1 of 3: Connection Name, Connection type and Pre-Shared Key
What is the new Connection Name?
Scenario_1
What is the pre-shared key?
12345678
This VPN tunnel will connect to.
A remote VPN Gateway
A remote VPN client
Back
Next
Cancel
VPN Wizard
Step 2 of 3: Remote VPN Gateway IP address or Internet name
What is the remote WAN's IP address or Internet name?
22.23.24.25
Back
Next
Cancel
VPN Wizard
Step 3 of 3: Secure Connection Remote Accessibility
What is the remote LAN IP subnet?
IP Address: 172 . 23 . 9 . 1
Subnet Mask: 255 . 255 . 255 . 0
Back
Next
Cancel

Continue as shown in Figure E-3

Gateway B VPN Parameter Entry


VPN Wizard
Step 1 of 3: Connection Name, Connection type and Pre-Shared Key
What is the new Connection Name?
Scenario_1
What is the pre-shared key?
12345678
This VPN tunnel will connect to.
A remote VPN Gateway
A remote VPN client
Back
Next
Cancel
VPN Wizard
Step 2 of 3: Remote VPN Gateway IP address or Internet name
What is the remote WAN's IP address or Internet name?
14.15.16.17
Back
Next
Cancel
VPN Wizard
Step 3 of 3: Secure Connection Remote Accessibility
What is the remote LAN IP subnet?
IP Address: 10 . 5 . 6 . 1
Subnet Mask: 255 . 255 . 255 . 0
Back
Next
Cancel

Continue as shown in Figure E-3

Figure E-11: VPN parameter entry at Gateway A (FVS318v3) and Gateway B (FVS318v2)

Viewing and Editing the VPN Parameters

The VPN Wizard sets up a VPN tunnel using the default parameters from the VPN Consortium (VPNC). The policy definitions to manage VPN traffic are presented in Figure E-12.

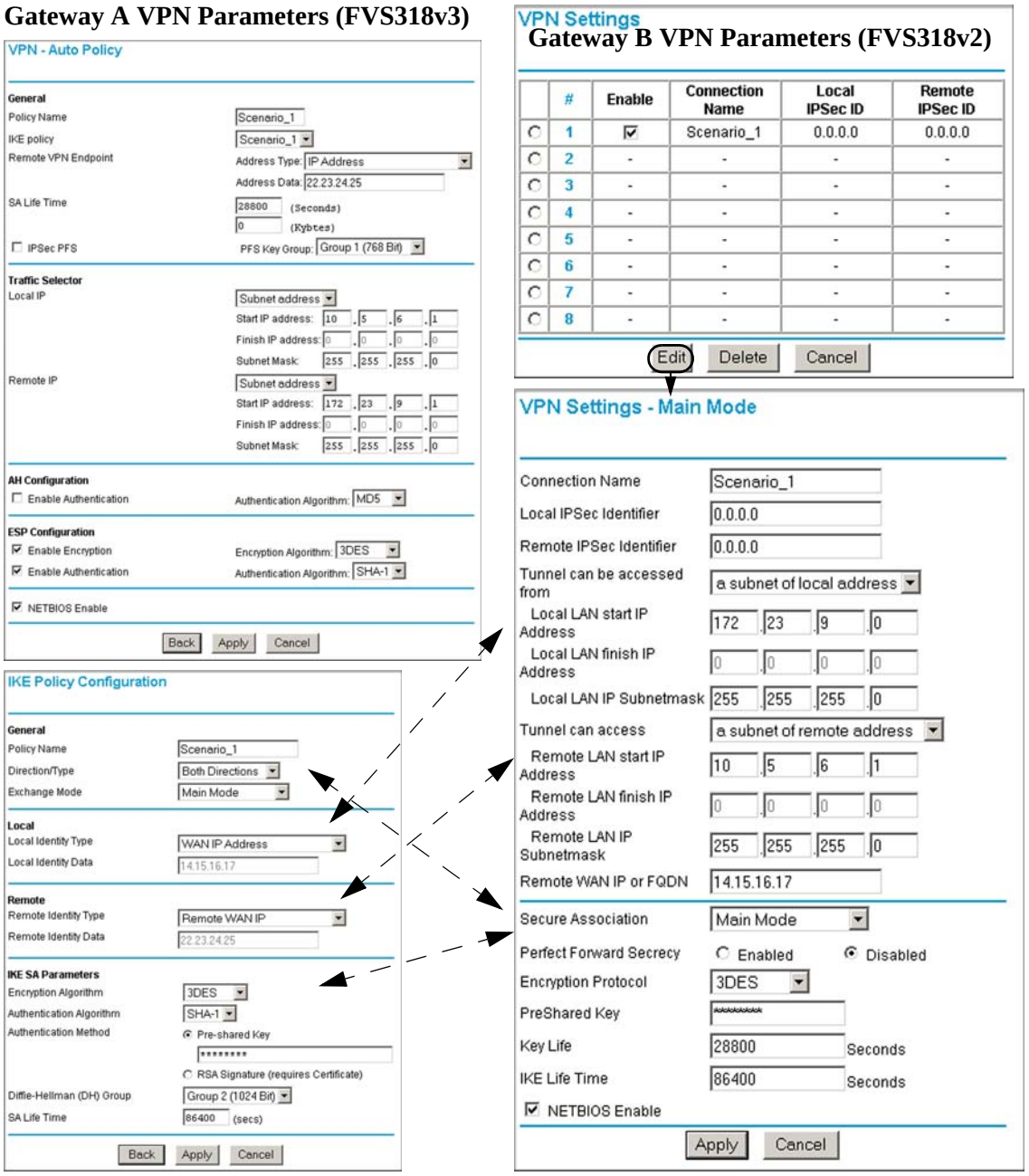


Figure E-12: VPN Parameters at Gateway A (FVS318v3) and Gateway B (FVS318v2)

	Note: The Pre-Shared Key must be the same at both VPN tunnel endpoints. The remote WAN and LAN IP addresses for one VPN tunnel endpoint will be the local WAN and LAN IP addresses for the other VPN tunnel endpoint. The VPN Wizard ensures the other VPN parameters are the same at both VPN tunnel endpoints.

Initiating and Checking the VPN Connections

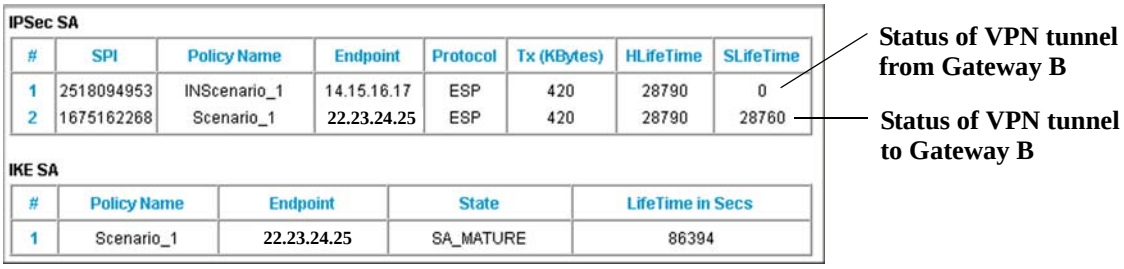
You can test connectivity and view VPN status information on the FVS318v3 according to the testing flowchart shown in Figure E-4. To test the VPN tunnel from the Gateway A LAN, do the following:

1. **Test 1: Ping Remote LAN IP Address**: To establish the connection between the FVS318v3 Gateway A and FVS318v2 Gateway B tunnel endpoints, perform these steps at Gateway A:
   a. From a Windows PC attached to the FVS318v3 on LAN A, click the **Start** button on the taskbar and then click **Run**.
   b. Type **ping -t 172.23.9.1**, and then click **OK** (you would type **ping -t 10.5.6.1** if testing from Gateway B).
   c. This will cause a continuous ping to be sent to the LAN interface of Gateway B. Within two minutes, the ping response should change from timed out to reply.

   At this point the VPN-tunnel-endpoint-to-VPN-tunnel-endpoint connection is established.
2. **Test 2: Ping Remote WAN IP Address (if Test 1 fails)**: To test connectivity between the Gateway A and Gateway B WAN ports, follow these steps:
   a. Log in to the router on LAN A, go to the main menu Maintenance section, and click the **Diagnostics** link.
   b. To test connectivity to the WAN port of Gateway B, enter **22.23.24.25**, and then click **Ping** (you would enter **14.15.16.17** if testing from Gateway B).
   c. This causes a ping to be sent to the WAN interface of Gateway B. Within two minutes, the ping response should change from timed out to reply. You may have to run this test several times before you get the reply message back from the target FVS318v2.
   d. At this point the gateway-to-gateway connection is verified.

3. **Test 3: View VPN Tunnel Status**: To view the FVS318v3 and FVS318v2 event log and status of Security Associations, go to the FVS318v3 main menu VPN section and click the **VPN Status** link. For the FVS318v2, click **Show VPN Status** from the Router Status screen.

VPN Status at Gateway A (FVS318v3)


IPSec SA
SPI Policy Name Endpoint Protocol Tx (KBytes) HLifeTime SLifeTime
1 2518094953 INScenario_1 14.15.16.17 ESP 420 28790 0
2 1675162268 Scenario_1 22.23.24.25 ESP 420 28790 28760
IKE SA
Policy Name Endpoint State LifeTime in Secs
1 Scenario_1 22.23.24.25 SA_MATURE 86394
Status of VPN tunnel from Gateway B
Status of VPN tunnel to Gateway B

IPSec Connection Status at Gateway B (FVS318v2)

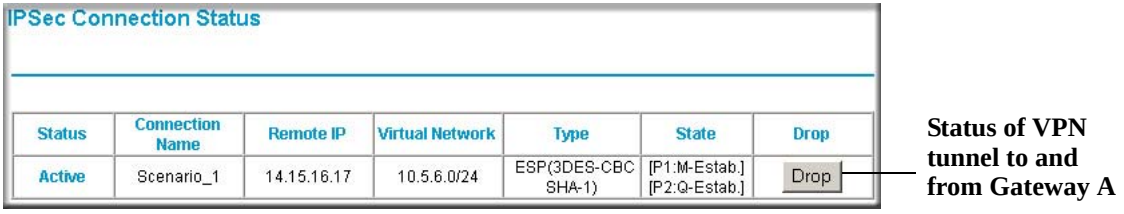

IPSec Connection Status
Status Connection Name Remote IP Virtual Network Type State Drop
Active Scenario_1 14.15.16.17 10.5.6.0/24 ESP(3DES-CBC SHA-1) [P1:M-Estab.] [P2:Q-Estab.] Drop
Status of VPN tunnel to and from Gateway A

Figure E-13: VPN Status for the routers at Gateway A (FVS318v3) and Gateway B (FVS318v2)

The FVS318v3-to-FVL328 Case

Table E-3. Policy Summary

VPN Consortium Scenario:		Scenario 1
Type of VPN		LAN-to-LAN or Gateway-to-Gateway
Security Scheme:		IKE with Preshared Secret/Key
Date Tested:		November 2004
Model/Firmware Tested:		
	NETGEAR-Gateway A	FVS318v3 with firmware version v3.0_14
	NETGEAR-Gateway B	FVL328 with firmware version V2.0_01
IP Addressing:		
	NETGEAR-Gateway A	Static IP address
	NETGEAR-Gateway B	Static IP address

Configuring the VPN Tunnel

Note: This scenario assumes all ports are open on the FVS318v3 and FVL328.

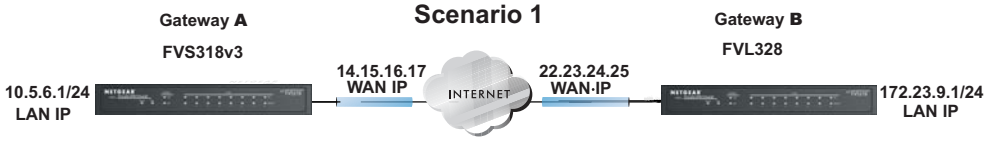


Figure E-14: LAN to LAN VPN access from an FVS318v3 to an FVL328

Use this scenario illustration and configuration screens as a model to build your configuration.

1. **Log in to the FVS318v3 labeled Gateway A as in the illustration (Figure E-14).**

   Log in at the default address of *http://192.168.0.1* with the default user name of **admin** and default password of **password** (or using whatever password and LAN address you have chosen).

Note: Based on the network addresses used in this example, you would log in to the LAN IP address of *http://10.5.6.1* at Gateway A.

2. Use the VPN Wizard to configure the FVS318v3 at Gateway A.

Follow the steps listed in Figure E-2 and Figure E-3 using the following parameters as illustrated in Figure E-15:

- Connection Name: **Scenario_1** (in this example)
- Pre-Shared Key: **12345678** (in this example), must be the same at both VPN tunnel endpoints
- Remote WAN IP address: **22.23.24.25** (in this example), must be unique at each VPN tunnel endpoint
- Remote LAN IP Subnet
  - IP Address: **172.23.9.1** (in this example), must be unique at each VPN tunnel endpoint
  - Subnet Mask: **255.255.255.0** (in this example)

3. **Log in to the FVL328 labeled Gateway B as in the illustration (Figure E-14).**

Log in at the default address of *http://192.168.0.1* with the default user name of **admin** and default password of **password** (or using whatever password and LAN address you have chosen).

Note: Based on the network addresses used in this example, you would log in to the LAN IP address of *http://172.23.9.1* at Gateway B.

4. Repeat the process using the VPN Wizard to configure the FVL328 at Gateway B.

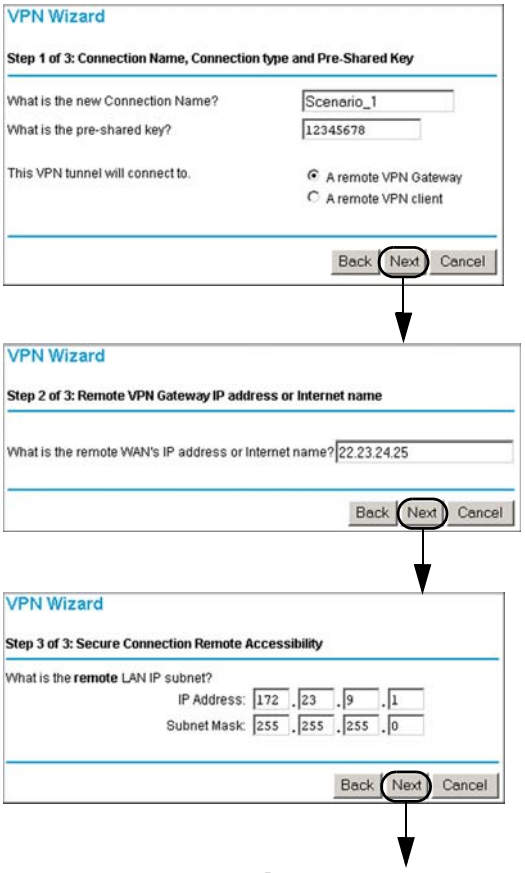
Follow the steps listed in Figure E-2 and Figure E-3, but use the following parameters instead as illustrated in Figure E-15:

- Connection Name: **Scenario_1** (in this example)
- Pre-Shared Key: **12345678** (in this example), must be the same at both VPN tunnel endpoints
- Remote WAN IP address: **14.15.16.17** (in this example), must be unique at each VPN tunnel endpoint

- Remote LAN IP Subnet
  - IP Address: **10.5.6.1** (in this example), must be unique at each VPN tunnel endpoint
  - Subnet Mask: **255.255.255.0** (in this example)

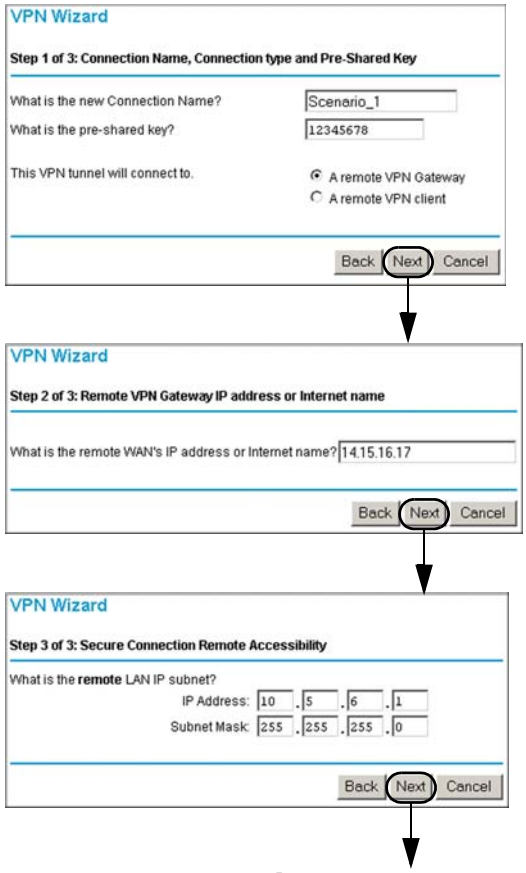
All traffic from the range of LAN IP addresses specified on FVS318v3 A and FVL328 B will now flow over a secure VPN tunnel once the VPN tunnel is initiated (see "Initiating and Checking the VPN Connections" on page 25).

Gateway A VPN Parameter Entry


VPN Wizard
Step 1 of 3: Connection Name, Connection type and Pre-Shared Key
What is the new Connection Name?
Scenario_1
What is the pre-shared key?
12345678
This VPN tunnel will connect to.
A remote VPN Gateway
A remote VPN client
Back
Next
Cancel
VPN Wizard
Step 2 of 3: Remote VPN Gateway IP address or Internet name
What is the remote WAN's IP address or Internet name?
22.23.24.25
Back
Next
Cancel
VPN Wizard
Step 3 of 3: Secure Connection Remote Accessibility
What is the remote LAN IP subnet?
IP Address: 172 . 23 . 9 . 1
Subnet Mask: 255 . 255 . 255 . 0
Back
Next
Cancel

Continue as shown in Figure E-3

Gateway B VPN Parameter Entry


VPN Wizard
Step 1 of 3: Connection Name, Connection type and Pre-Shared Key
What is the new Connection Name?
Scenario_1
What is the pre-shared key?
12345678
This VPN tunnel will connect to.
A remote VPN Gateway
A remote VPN client
Back
Next
Cancel
VPN Wizard
Step 2 of 3: Remote VPN Gateway IP address or Internet name
What is the remote WAN's IP address or Internet name?
14.15.16.17
Back
Next
Cancel
VPN Wizard
Step 3 of 3: Secure Connection Remote Accessibility
What is the remote LAN IP subnet?
IP Address: 10 . 5 . 6 . 1
Subnet Mask: 255 . 255 . 255 . 0
Back
Next
Cancel

Continue as shown in Figure E-3

Figure E-15: VPN parameter entry at Gateway A (FVS318v3) and Gateway B (FVL328)

Viewing and Editing the VPN Parameters

The VPN Wizard sets up a VPN tunnel using the default parameters from the VPN Consortium (VPNC). The policy definitions to manage VPN traffic on the FVS318v3 and FVL328 are presented in Figure E-16 and Figure E-17.

Gateway A VPN Policy Parameters **Gateway B VPN Policy Parameters**

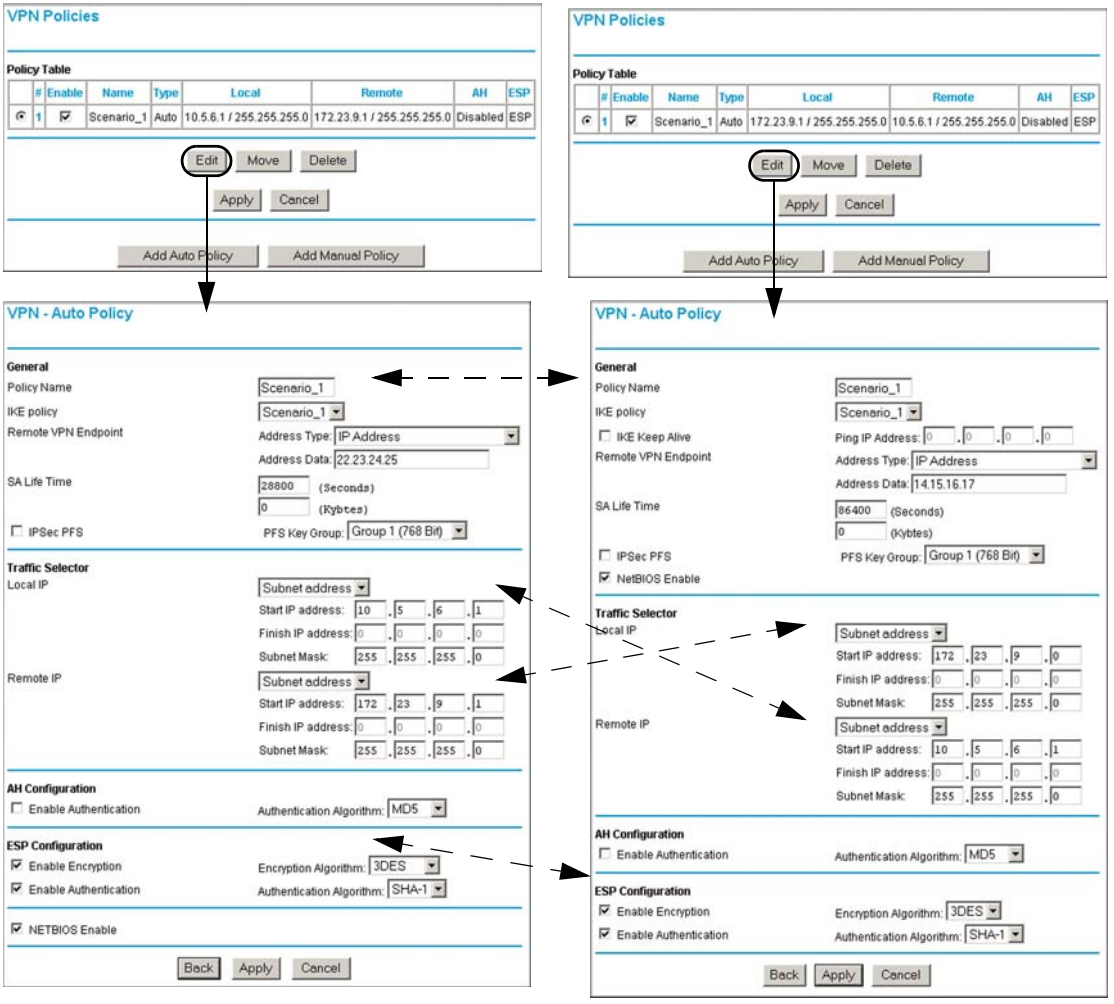

VPN Policies
Policy Table
Enable Name Type Local Remote AH ESP
1 Scenario_1 Auto 10.5.6.1 / 255.255.255.0 172.23.9.1 / 255.255.255.0 Disabled ESP
Edit Move Delete
Apply Cancel
Add Auto Policy Add Manual Policy
VPN - Auto Policy
General
Policy Name Scenario_1
IKE policy Scenario_1
Remote VPN Endpoint Address Type: IP Address
Address Data: 22.23.24.25
SA Life Time 28800 (Seconds)
0 (Kybtes)
IPSec PFS PFS Key Group: Group 1 (768 Bit)
Traffic Selector
Local IP Subnet address
Start IP address: 10.5.6.1
Finish IP address: 0.0.0.0
Subnet Mask: 255.255.255.0
Remote IP Subnet address
Start IP address: 172.23.9.1
Finish IP address: 0.0.0.0
Subnet Mask: 255.255.255.0
AH Configuration
Enable Authentication Authentication Algorithm: MD5
ESP Configuration
Enable Encryption Encryption Algorithm: 3DES
Enable Authentication Authentication Algorithm: SHA-1
NETBIOS Enable
Back Apply Cancel
VPN Policies
Policy Table
Enable Name Type Local Remote AH ESP
1 Scenario_1 Auto 172.23.9.1 / 255.255.255.0 10.5.6.1 / 255.255.255.0 Disabled ESP
Edit Move Delete
Apply Cancel
Add Auto Policy Add Manual Policy
VPN - Auto Policy
General
Policy Name Scenario_1
IKE policy Scenario_1
IKE Keep Alive Ping IP Address: 0.0.0.0
Remote VPN Endpoint Address Type: IP Address
Address Data: 14.15.16.17
SA Life Time 86400 (Seconds)
0 (Kybtes)
IPSec PFS PFS Key Group: Group 1 (768 Bit)
NetBIOS Enable
Traffic Selector
Local IP Subnet address
Start IP address: 172.23.9.0
Finish IP address: 0.0.0.0
Subnet Mask: 255.255.255.0
Remote IP Subnet address
Start IP address: 10.5.6.1
Finish IP address: 0.0.0.0
Subnet Mask: 255.255.255.0
AH Configuration
Enable Authentication Authentication Algorithm: MD5
ESP Configuration
Enable Encryption Encryption Algorithm: 3DES
Enable Authentication Authentication Algorithm: SHA-1
Back Apply Cancel

Figure E-16: VPN policies at Gateway A (FVS318v3) and Gateway B (FVL328)

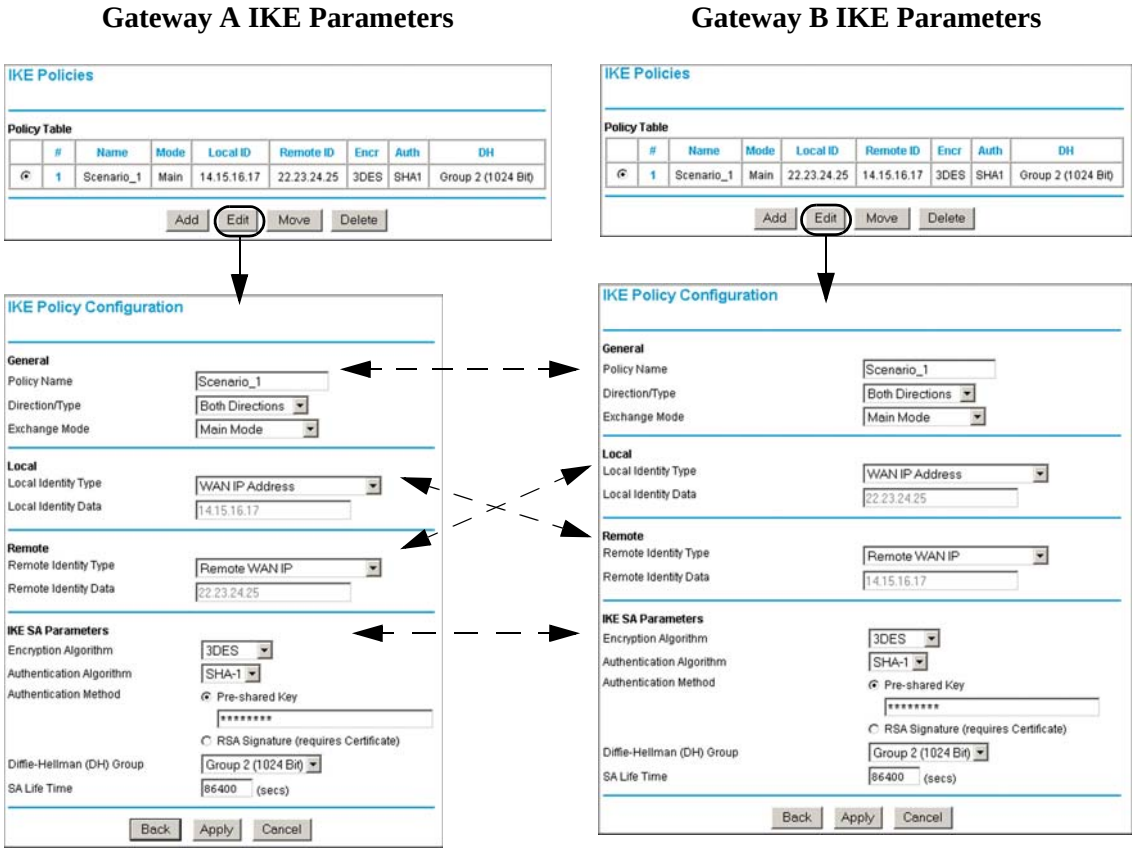


Figure E-17: IKE parameters at Gateway A (FVS318v3) and Gateway B (FVL328)

Note: The Pre-Shared Key must be the same at both VPN tunnel endpoints.

The remote WAN and LAN IP addresses for one VPN tunnel endpoint will be the local WAN and LAN IP addresses for the other VPN tunnel endpoint.

The VPN Wizard ensures the other VPN parameters are the same at both VPN tunnel endpoints.

Initiating and Checking the VPN Connections

You can test connectivity and view VPN status information on the FVS318v3 and FVL328 according to the testing flowchart shown in Figure E-4. To test the VPN tunnel from the Gateway A LAN, do the following:

1. **Test 1: Ping Remote LAN IP Address**: To establish the connection between the FVS318v3 Gateway A and FVL328 Gateway B tunnel endpoints, perform these steps at Gateway A:

   a. From a Windows PC attached to the FVS318v3 on LAN A, click the **Start** button on the taskbar and then click **Run**.

   b. Type **ping -t 172.23.9.1**, and then click **OK** (you would type **ping -t 10.5.6.1** if testing from Gateway B).

   c. This will cause a continuous ping to be sent to the LAN interface of Gateway B. Within two minutes, the ping response should change from timed out to reply.

   At this point the VPN-tunnel-endpoint-to-VPN-tunnel-endpoint connection is established.

2. **Test 2: Ping Remote WAN IP Address (if Test 1 fails)**: To test connectivity between the Gateway A and Gateway B WAN ports, follow these steps:

   a. Log in to the router on LAN A, go to the main menu Maintenance section, and click the **Diagnostics** link.

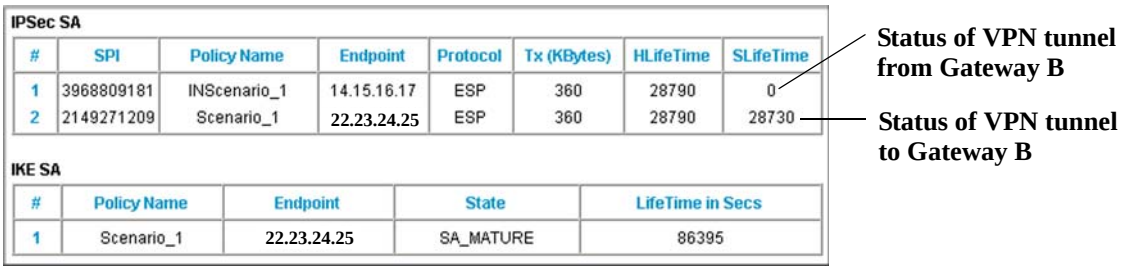
   b. To test connectivity to the WAN port of Gateway B, enter **22.23.24.25**, and then click **Ping** (you would enter **14.15.16.17** if testing from Gateway B).

   c. This causes a ping to be sent to the WAN interface of Gateway B. Within two minutes, the ping response should change from timed out to reply. You may have to run this test several times before you get the reply message back from the target FVL328.

   d. At this point the gateway-to-gateway connection is verified.

3. **Test 3: View VPN Tunnel Status**: To view the FVS318v3 and FVL328 event log and status of Security Associations, go to the FVS318v3 main menu VPN section and click the **VPN Status** link. For the FVL328, click **VPN Status** on the VPN Status/Log screen.

VPN Status at Gateway A (FVS318v3)



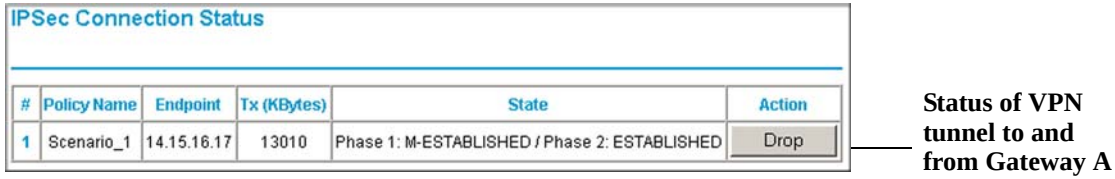
IPSec SA

#	SPI	Policy Name	Endpoint	Protocol	Tx (KBytes)	HLifeTime	SLifeTime
1	3968809181	INScenario_1	14.15.16.17	ESP	360	28790	0
2	2149271209	Scenario_1	22.23.24.25	ESP	360	28790	28730

IKE SA

#	Policy Name	Endpoint	State	LifeTime in Secs
1	Scenario_1	22.23.24.25	SA_MATURE	86395

IPSec Connection Status at Gateway B (FVL328)



IPSec Connection Status

#	Policy Name	Endpoint	Tx (KBytes)	State	Action
1	Scenario_1	14.15.16.17	13010	Phase 1: M-ESTABLISHED / Phase 2: ESTABLISHED	Drop

Figure E-18: VPN Status for the routers at Gateway A (FVS318v3) and Gateway B (FVL328)

The FVS318v3-to-VPN Client Case

Table E-4. Policy Summary

VPN Consortium Scenario:		Scenario 1
Type of VPN		PC/Client-to-Gateway
Security Scheme:		IKE with Preshared Secret/Key
Date Tested:		November 2004
Model/Firmware Tested:		
	NETGEAR-Gateway A	FVS318v3 with firmware version v3.0_14
	NETGEAR-Client B	NETGEAR ProSafe VPN Client v10.3.5
IP Addressing:		
	NETGEAR-Gateway A	Static IP address
	NETGEAR-Client B	Dynamic IP address

Client-to-Gateway VPN Tunnel Overview

The operational differences between gateway-to-gateway and client-to-gateway VPN tunnels are summarized as follows:

Table E-5. Differences between VPN tunnel types

Operation	Gateway-to-Gateway VPN Tunnels	Client-to-Gateway VPN Tunnels
Exchange Mode	**Main Mode**—The IP addresses of both gateways are known (especially when FQDN is used), so each gateway can use the Internet source of the traffic for validation purposes.	**Aggressive Mode**—The IP address of the client is not known in advance, so the gateway is programmed to accept valid traffic sourced from any Internet location (i.e., less secure).
Direction/Type	**Both Directions**—Either end of the VPN tunnel may initiate traffic (usually).	**Remote Access**—The client end of the VPN tunnel must initiate traffic because its IP address is not know in advance, which prevents the gateway end of the VPN tunnel from initiating traffic.

Configuring the VPN Tunnel

Note: This scenario assumes all ports are open on the FVS318v3.

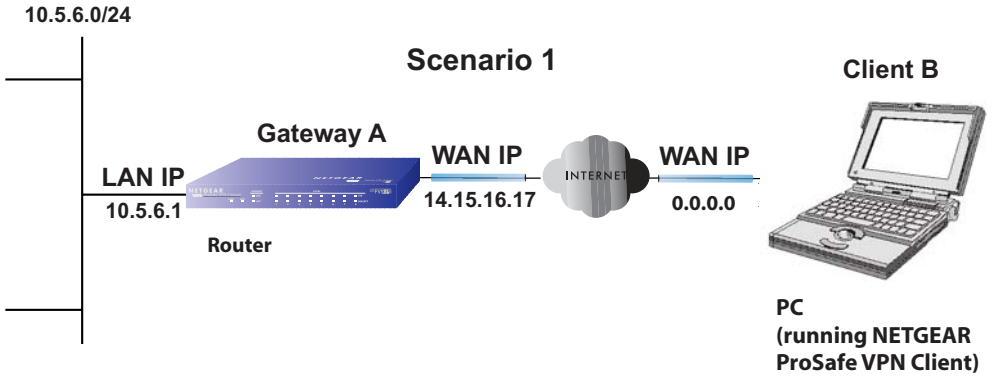


Figure E-19: LAN to PC VPN access from an FVS318v3 to a VPN Client

Use this scenario illustration and configuration screens as a model to build your configuration.

1. **Log in to the FVS318v3 labeled Gateway A as in the illustration (Figure E-19).**

   Log in at the default address of *http://192.168.0.1* with the default user name of **admin** and default password of **password** (or using whatever password and LAN address you have chosen).

	Note: Based on the network addresses used in this example, you would log in to the LAN IP address of *http://10.5.6.1* at Gateway A.

2. **Use the VPN Wizard to configure the FVS318v3 at Gateway A.**

   Follow the steps illustrated in Figure E-19 (the resulting parameter screens are shown in Figure E-20):

   - Connection Name: **Scenario_1** (in this example)
   - Pre-Shared Key: **12345678** (in this example), must be the same at both VPN tunnel endpoints
   - Connection Type: **A Remote VPN Client**

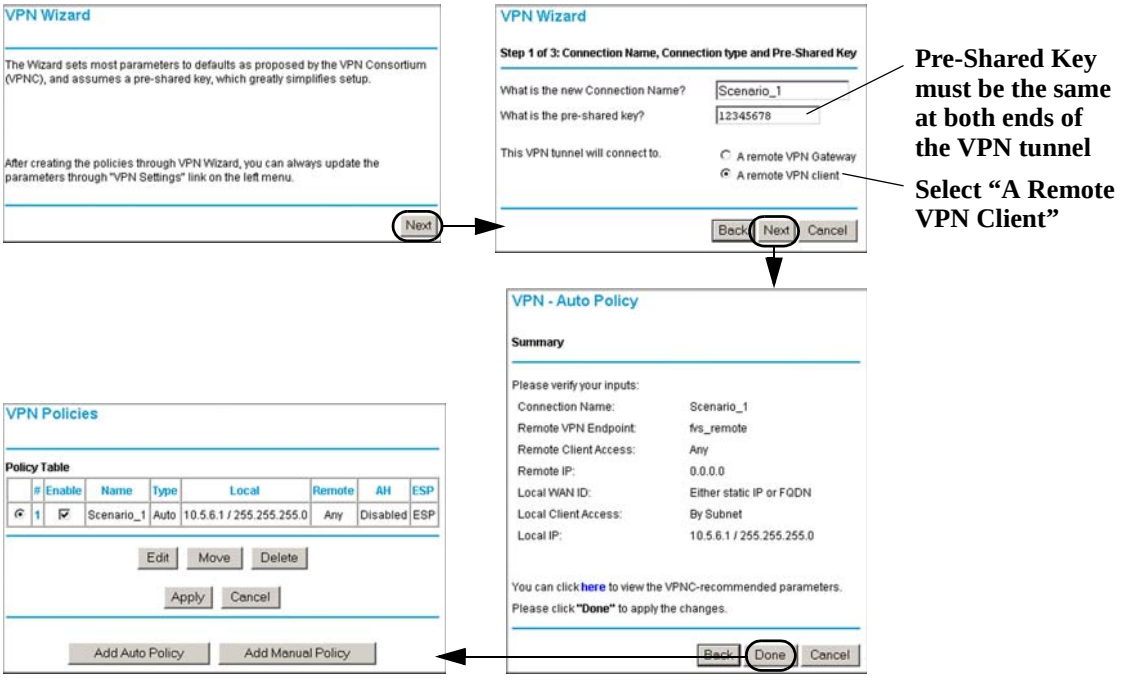

VPN Wizard
The Wizard sets most parameters to defaults as proposed by the VPN Consortium (VPNC), and assumes a pre-shared key, which greatly simplifies setup.
After creating the policies through VPN Wizard, you can always update the parameters through "VPN Settings" link on the left menu.
Next
VPN Wizard
Step 1 of 3: Connection Name, Connection type and Pre-Shared Key
What is the new Connection Name?
Scenario_1
What is the pre-shared key?
12345678
This VPN tunnel will connect to.
A remote VPN Gateway
A remote VPN client
Back
Next
Cancel
Pre-Shared Key must be the same at both ends of the VPN tunnel
Select "A Remote VPN Client"
VPN - Auto Policy
Summary
Please verify your inputs:
Connection Name: Scenario_1
Remote VPN Endpoint: fvs_remote
Remote Client Access: Any
Remote IP: 0.0.0.0
Local WAN ID: Either static IP or FQDN
Local Client Access: By Subnet
Local IP: 10.5.6.1 / 255.255.255.0
You can click here to view the VPNC-recommended parameters.
Please click "Done" to apply the changes.
Back
Done
Cancel
VPN Policies
Policy Table
Enable Name Type Local Remote AH ESP
1 Scenario_1 Auto 10.5.6.1 / 255.255.255.0 Any Disabled ESP
Edit
Move
Delete
Apply
Cancel
Add Auto Policy
Add Manual Policy

Figure E-20: VPN Wizard at Gateway A (FVS318v3)

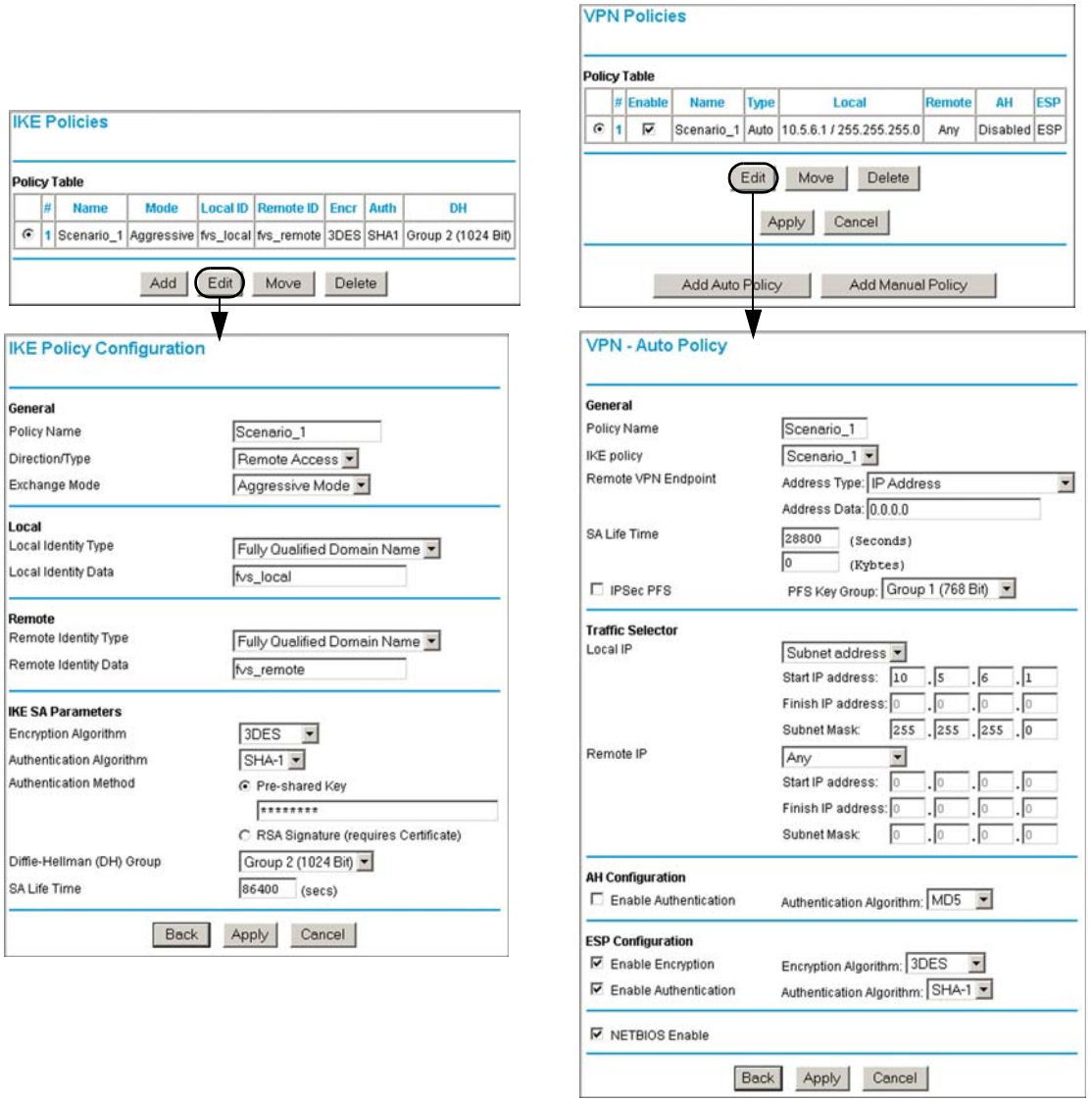

IKE Policies
Policy Table
Name Mode Local ID Remote ID Encr Auth DH
1 Scenario_1 Aggressive fvs_local fvs_remote 3DES SHA1 Group 2 (1024 Bit)
Add Edit Move Delete
IKE Policy Configuration
General
Policy Name Scenario_1
Direction/Type Remote Access
Exchange Mode Aggressive Mode
Local
Local Identity Type Fully Qualified Domain Name
Local Identity Data fvs_local
Remote
Remote Identity Type Fully Qualified Domain Name
Remote Identity Data fvs_remote
IKE SA Parameters
Encryption Algorithm 3DES
Authentication Algorithm SHA-1
Authentication Method Pre-shared Key
RSA Signature (requires Certificate)
Diffie-Hellman (DH) Group Group 2 (1024 Bit)
SA Life Time 86400 (secs)
Back Apply Cancel
VPN Policies
Policy Table
Enable Name Type Local Remote AH ESP
1 Scenario_1 Auto 10.5.6.1 / 255.255.255.0 Any Disabled ESP
Edit Move Delete
Apply Cancel
Add Auto Policy Add Manual Policy
VPN - Auto Policy
General
Policy Name Scenario_1
IKE policy Scenario_1
Remote VPN Endpoint Address Type: IP Address
Address Data: 0.0.0.0
SA Life Time 28800 (Seconds)
0 (Kybtes)
IPSec PFS PFS Key Group: Group 1 (768 Bit)
Traffic Selector
Local IP Subnet address
Start IP address: 10 . 5 . 6 . 1
Finish IP address: 0 . 0 . 0 . 0
Subnet Mask: 255 . 255 . 255 . 0
Remote IP Any
Start IP address: 0 . 0 . 0 . 0
Finish IP address: 0 . 0 . 0 . 0
Subnet Mask: 0 . 0 . 0 . 0
AH Configuration
Enable Authentication Authentication Algorithm: MD5
ESP Configuration
Enable Encryption Encryption Algorithm: 3DES
Enable Authentication Authentication Algorithm: SHA-1
NETBIOS Enable
Back Apply Cancel

Figure E-21: VPN parameters at Gateway A (FVS318v3)

3. **Set up the VPN Client at Gateway B as in the illustration (Figure E-19).**

   a. Right-mouse-click the ProSafe icon ( ) in the system tray and select the Security Policy Editor. If you need to install the NETGEAR ProSafe VPN Client on your PC, consult the documentation that came with your software.

   b. Add a new connection using the Edit/Add/Connection menu and rename it **Scenario_1**. (**Scenario_1** is used in this example to reflect the fact that the connection uses the Pre-Shared Key security scheme and encryption parameters proposed by the VPN Consortium, but you may want to choose a name for your connection that is meaningful to your specific installation. The name you choose does not have to match the name used at the gateway end of the VPN tunnel.)

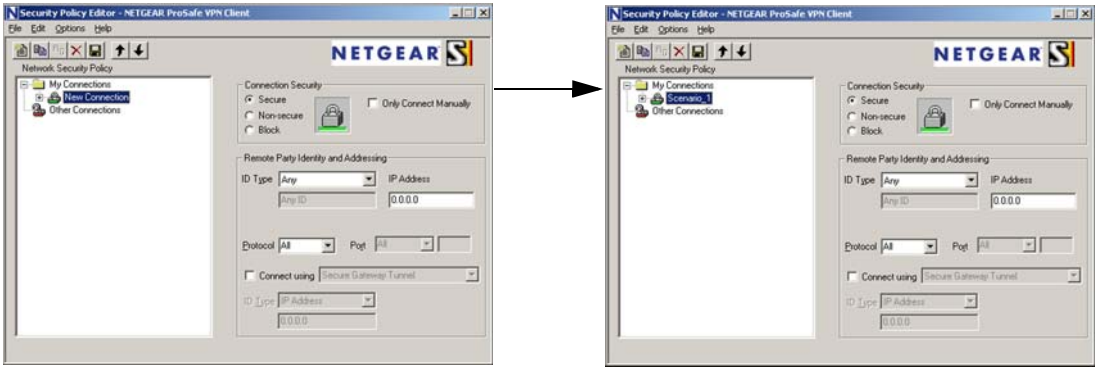


Figure E-22: Adding and renaming a new connection

c. Program the **Scenario_1** connection screen as follows (see Figure E-23):

- Connection Security: **Secure**
- Remote Party Identity and Addressing: Select **IP Subnet** from the ID Type menu and then enter **10.5.6.1** for **Subnet**, **255.255.255.0** for **Mask**, and leave **All** for **Protocol**. (The **Subnet** and **Mask** parameters entered here must match the **Start IP address** and **Subnet Mask** parameters of the **Local IP Traffic Selector** on the **VPN Autopolicy** screen shown in Figure E-21 for the gateway router.)
- Enable **Connect Using Secure Gateway Tunnel**; select **Domain Name** for **ID_Type**; enter **fvs_local** for **Domain Name**; and enter **14.15.16.17** for **Gateway IP Address**. (**Domain Name** must match the **Local Identity Data** parameter of the **IKE Policy Configuration** screen shown in Figure E-21 for the gateway router. Also, **Gateway IP Address** must match the WAN IP address of the gateway router shown in Figure E-19.)
- Expand the Scenario_1 screen hierarchy by clicking the + sign in front of Scenario_1. Then expand the rest of the screen hierarchies by clicking the rest of the + signs.

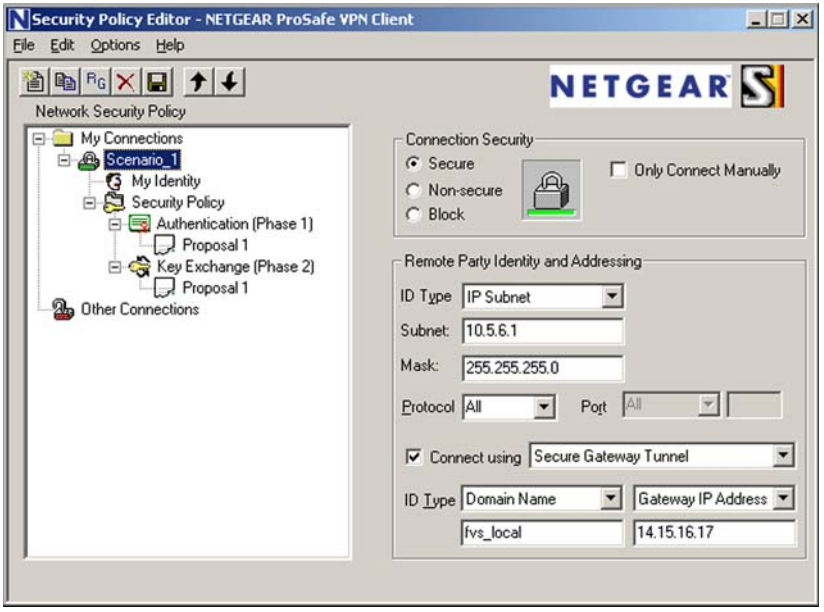


Figure E-23: Scenario_1 connection screen parameters

d. Select **Security Policy** on the left hierarchy menu and then select **Aggressive Mode** under **Select Phase 1 Negotiation Mode** (see Figure E-24). (The **Select Phase 1 Negotiation Mode** choice must match the **Exchange Mode** setting for the **General IKE Policy Configuration** parameters shown in Figure E-21 for the gateway router.)

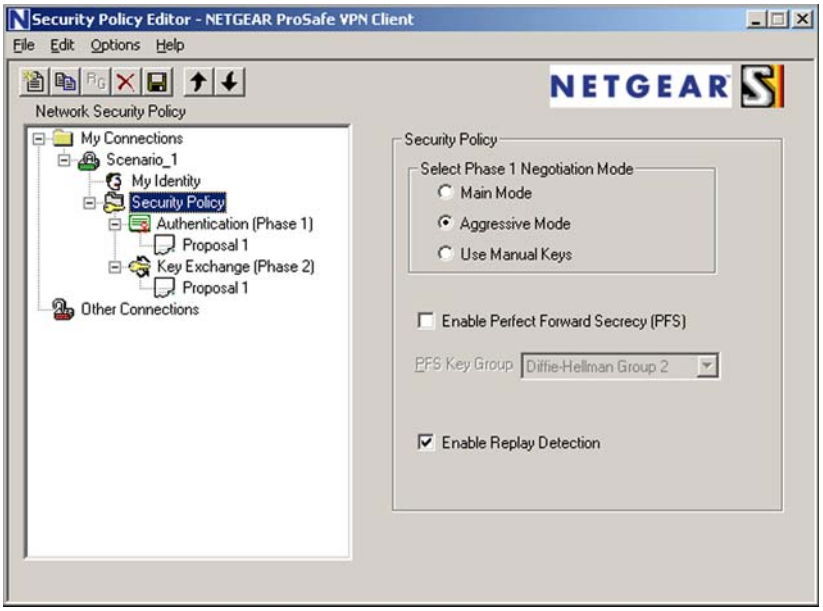


Figure E-24: Scenario_1 Security Policy screen parameters

e. Select My Identity on the left hierarchy menu and program the screen as follows (see Figure E-25):

- Under **My Identity**, select **None** for **Select Certificate** (since we are using a Pre-Shared Key in this scenario). Then enter **12345678** for the **Pre-Shared Key** value. (The **Preshared-Key** value must match the value you entered in the VPN Wizard for the gateway **Pre-Shared Key** value shown in Figure E-20.)
- Under **My Identity**, select **Domain Name** for the **ID Type** and then enter **fvs_remote**. (**Domain Name** must match the **Remote Identity Data** parameter of the **IKE Policy Configuration** screen shown in Figure E-21 for the gateway router.)

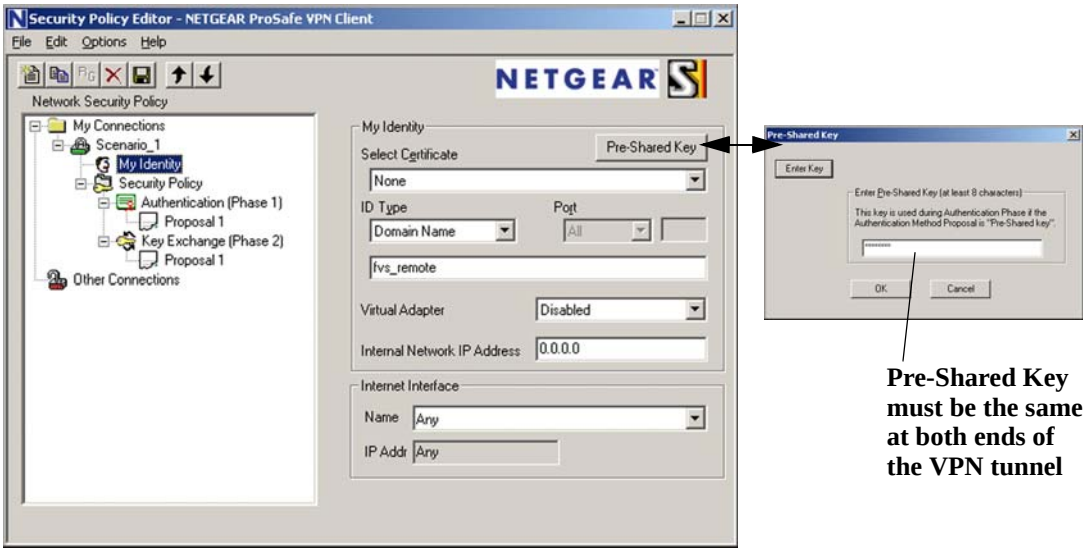


Figure E-25: Scenario_1 My Identity screen parameters

f. Verify the **Authentication (Phase 1)** and **Key Exchange (Phase 1) Proposal 1** screen parameters (see Figure E-26) match the **IKE SA Parameters** of the **IKE Policy Configuration** screen shown in Figure E-21 for the gateway router.

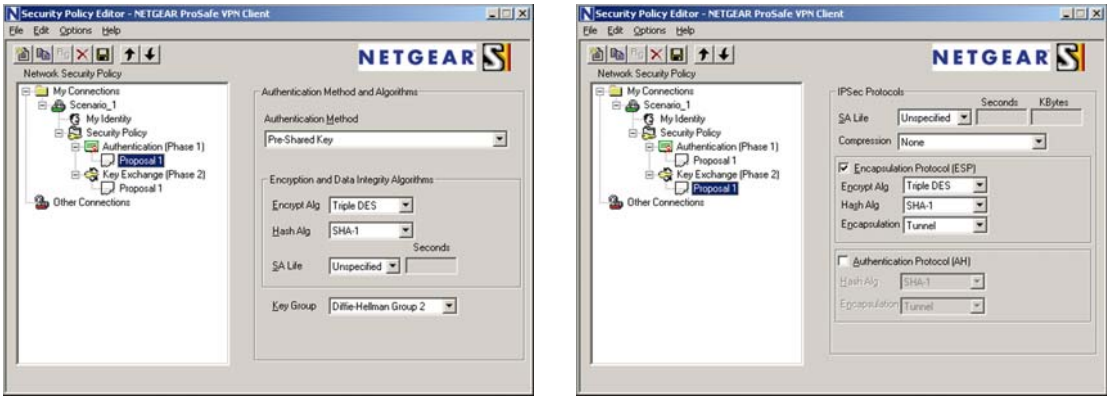


Figure E-26: Scenario_1 Proposal 1 parameters for Authentication and Key Exchange

g. Save the **Scenario_1** connection using Save under the File menu. You can also export the connection parameters using Export Security Policy under the File menu.

You are new ready to activate the tunnel, but you must do it from the client endpoint (see "Initiating and Checking the VPN Connections" on page 36). In the client-to-gateway scenario, the gateway router will not know the client's IP address until the client initiates the traffic.

Initiating and Checking the VPN Connections

You can test connectivity and view VPN status information on the FVS318v3 and VPN Client according to the testing flowchart shown in Figure E-4. To test the VPN tunnel from the Gateway A LAN, do the following:

1. **Test 1: Launch Scenario_1 Connection from Client PC**: To check the **VPN Connection**, you can initiate a request from the remote PC to the VPN router's network by using the **Connect** option in the VPN Client's menu bar (see Figure E-27). Since the remote PC has a dynamically assigned WAN IP address, it must initiate the request.

   a. Open the popup menu by right-clicking on the system tray icon.

   b. Select **Connect** to open the **My Connections** list.

   c. Choose **Scenario_1**.

   The VPN Client reports the results of the attempt to connect. Once the connection is established, you can access resources of the network connected to the VPN router.

   Alternative Ping Test: To perform a ping test as an alternative, start from the remote PC:

   a. From a Windows Client PC, click the **Start** button on the taskbar and then click **Run**.

   b. Type **ping -t 10.5.6.1**, and then click **OK**.

   c. This will cause a continuous ping to be sent to the LAN interface of Gateway A. Within two minutes, the ping response should change from timed out to reply.

   At this point the VPN-tunnel-endpoint-to-VPN-tunnel-endpoint connection is established.

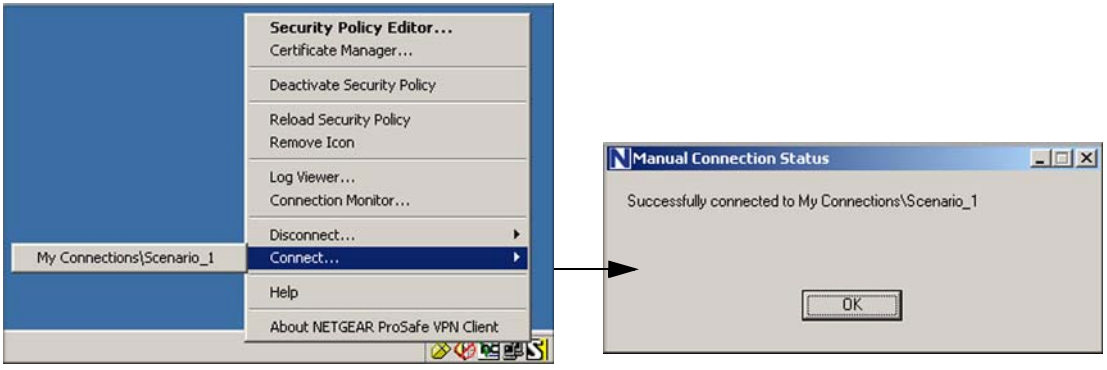


Figure E-27: Scenario_1 connection launch from VPN Client PC

2. **Test 2: Ping Remote WAN IP Address (if Test 1 fails)**: To test connectivity between the Gateway A and Gateway B WAN ports, follow these steps:

   a. From a Windows Client PC, click the **Start** button on the taskbar and then click **Run**.

   b. Type **ping -t 14.151.6.17**, and then click **OK**.

   c. This causes a ping to be sent to the WAN interface of Gateway A. Within two minutes, the ping response should change from timed out to reply. You may have to run this test several times before you get the reply message back from the target FVS318v3.

   d. At this point the gateway-to-gateway connection is verified.

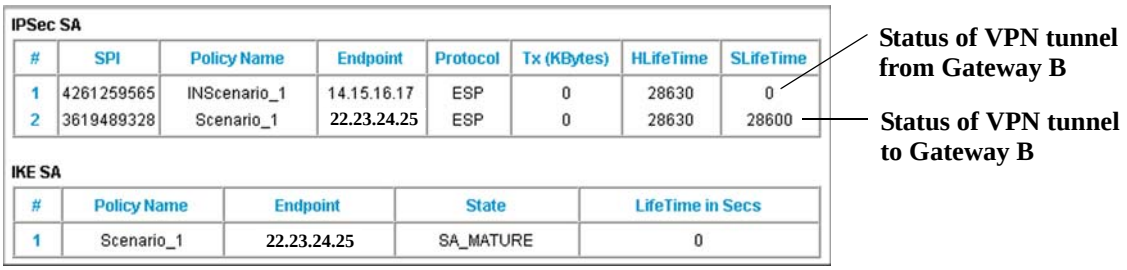
3. **Test 3: View VPN Tunnel Status**: To view the FVS318v3 event log and status of Security Associations, go to the FVS318v3 main menu VPN section and click the **VPN Status** link. For the For the VPN Client, click **VPN Status** on the VPN Status/Log screen.

   a. Open the popup menu by right-clicking on the system tray icon.

   b. Select **Connection Monitor**.

   See Figure E-28 for the resulting status screens.

VPN Status at Gateway A (FVS318v3)



IPSec SA

#	SPI	Policy Name	Endpoint	Protocol	Tx (KBytes)	HLifeTime	SLifeTime
1	4261259565	INScenario_1	14.15.16.17	ESP	0	28630	0
2	3619489328	Scenario_1	22.23.24.25	ESP	0	28630	28600

IKE SA

#	Policy Name	Endpoint	State	LifeTime in Secs
1	Scenario_1	22.23.24.25	SA_MATURE	0

Connection Monitor at Gateway B (remote VPN Client)

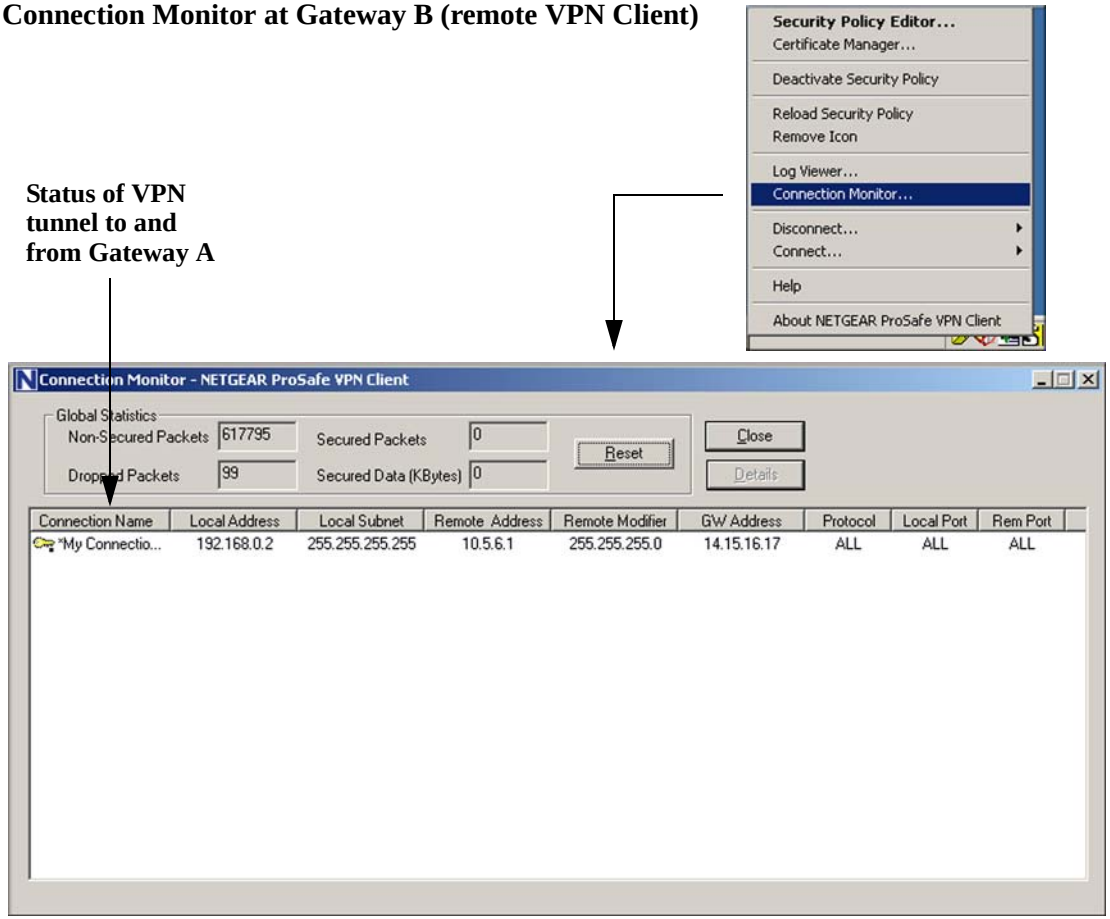


Figure E-28: VPN Status for Gateway A (FVS318v3) and Gateway B (VPN Client)

Glossary

List of Glossary Terms

Use the list below to find definitions for technical terms used in this manual.

Numeric

10BASE-T
IEEE 802.3 specification for 10 Mbps Ethernet over twisted pair wiring.

100BASE-Tx
IEEE 802.3 specification for 100 Mbps Ethernet over twisted pair wiring.

802.1x
802.1x defines port-based, network access control used to provide authenticated network access and automated data encryption key management. The IEEE 802.1x draft standard offers an effective framework for authenticating and controlling user traffic to a protected network, as well as dynamically varying encryption keys. 802.1x uses a protocol called EAP (Extensible Authentication Protocol) and supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, and public key authentication. For details on EAP specifically, refer to IETF's RFC 2284.

A

Access Control List (ACL)
An ACL is a database that an Operating System uses to track each user’s access rights to system objects (such as file directories and/or files).

ADSL
Short for asymmetric digital subscriber line, a technology that allows data to be sent over existing copper telephone lines at data rates of from 1.5 to 9 Mbps when receiving data (known as the downstream rate) and from 16 to 640 Kbps when sending data (known as the upstream rate). ADSL requires a special ADSL modem. ADSL is growing in popularity as more areas around the world gain access.

ARP
Address Resolution Protocol, a TCP/IP protocol used to convert an IP address into a physical address (called a DLC address), such as an Ethernet address. A host wishing to obtain a physical address broadcasts an ARP request onto the TCP/IP network. The host on the network that has the IP address in the request then replies with its physical hardware address. There is also Reverse ARP (RARP) which can be used by a host to discover its IP address. In this case, the host broadcasts its physical address and a RARP server replies with the host's IP address.

Auto Uplink
Auto Uplink™ technology (also called MDI/MDIX) eliminates the need to worry about crossover vs. straight-through Ethernet cables. Auto Uplink™ will accommodate either type of cable to make the right connection.

B

Bandwidth
The information capacity, measured in bits per second, that a channel could transmit. Bandwidth examples include 10 Mbps for Ethernet, 100 Mbps for Fast Ethernet, and 1000 Mbps (I Gbps) for Gigabit Ethernet.

Baud
The signaling rate of a line, that is, the number of transitions (voltage or frequency changes) made per second. Also known as line speed.

Broadcast
A packet sent to all devices on a network.

C

Class of Service
A term to describe treating different types of traffic with different levels of service priority. Higher priority traffic gets faster treatment during times of switch congestion

CA
A Certificate Authority is a trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs.

Cat 5
Category 5 unshielded twisted pair (UTP) cabling. An Ethernet network operating at 10 Mbits/second (10BASE-T) will often tolerate low quality cables, but at 100 Mbits/second (10BASE-Tx) the cable must be rated as Category 5, or Cat 5 or Cat V, by the Electronic Industry Association (EIA). This rating will be

printed on the cable jacket. Cat 5 cable contains eight conductors, arranged in four twisted pairs, and terminated with an RJ45 type connector. In addition, there are restrictions on maximum cable length for both 10 and 100 Mbits/second networks.

Certificate Authority

A Certificate Authority is a trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs. The role of the CA in this process is to guarantee that the individual granted the unique certificate is, in fact, who he or she claims to be. Usually, this means that the CA has an arrangement with a financial institution, such as a credit card company, which provides it with information to confirm an individual's claimed identity. CAs are a critical component in data security and electronic commerce because they guarantee that the two parties exchanging information are really who they claim to be.

D

DHCP

An Ethernet protocol specifying how a centralized DHCP server can assign network configuration information to multiple DHCP clients. The assigned information includes IP addresses, DNS addresses, and gateway (router) addresses.

DMZ

Specifying a Default DMZ Server allows you to set up a computer or server that is available to anyone on the Internet for services that you haven't defined. There are security issues with doing this, so only do this if you'll willing to risk open access.

DNS

Short for Domain Name System (or Service), an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4. The DNS system is, in fact, its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

Domain Name

A descriptive name for an address or group of addresses on the Internet. Domain names are of the form of a registered entity name plus one of a number of predefined top level suffixes such as .com, .edu, .uk, etc. For example, in the address mail.NETGEAR.com, mail is a server name and NETGEAR.com is the domain.

DSL

Short for digital subscriber line, but is commonly used in reference to the asymmetric version of this technology (ADSL) that allows data to be sent over existing copper telephone lines at data rates of from 1.5

to 9 Mbps when receiving data (known as the downstream rate) and from 16 to 640 Kbps when sending data (known as the upstream rate).
ADSL requires a special ADSL modem. ADSL is growing in popularity as more areas around the world gain access.

DSLAM
DSL Access Multiplexor. The piece of equipment at the telephone company central office that provides the ADSL signal.

Dynamic Host Configuration Protocol
DHCP. An Ethernet protocol specifying how a centralized DHCP server can assign network configuration information to multiple DHCP clients. The assigned information includes IP addresses, DNS addresses, and gateway (router) addresses.

E

EAP
Extensible Authentication Protocol is a general protocol for authentication that supports multiple authentication methods. EAP, an extension to PPP, supports such authentication methods as token cards, Kerberos, one-time passwords, certificates, public key authentication and smart cards. EAP is defined by RFC 2284.

Ethernet
A LAN specification developed jointly by Xerox, Intel and Digital Equipment Corporation. Ethernet networks transmit packets at a rate of 10 Mbps.

G

Gateway
A local device, usually a router, that connects hosts on a local network to other networks.

I

ICMP
See “Internet Control Message Protocol”

IEEE
Institute of Electrical and Electronics Engineers. This American organization was founded in 1963 and sets standards for computers and communications.

IETF
Internet Engineering Task Force. An organization responsible for providing engineering solutions for TCP/IP networks. In the network management area, this group is responsible for the development of the SNMP protocol.

IKE
Internet Key Exchange. An automated method for exchanging and managing encryption keys between two VPN devices.

Internet Control Message Protocol
ICMP is an extension to the Internet Protocol (IP) that supports packets containing error, control, and informational messages. The PING command, for example, uses ICMP to test an Internet connection.

Internet Protocol
The method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it among all other computers on the Internet. When you send or receive data (for example, an e-mail note or a Web page), the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. Any packet is sent first to a gateway computer that understands a small part of the Internet. The gateway computer reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the Internet until one gateway recognizes the packet as belonging to a computer within its immediate neighborhood or domain. That gateway then forwards the packet directly to the computer whose address is specified.

Because a message is divided into a number of packets, each packet can, if necessary, be sent by a different route across the Internet. Packets can arrive in a different order than they were sent. The Internet Protocol just delivers them. It's up to another protocol, the Transmission Control Protocol (TCP) to put them back in the right order. IP is a connectionless protocol, which means that there is no continuing connection between the end points that are communicating. Each packet that travels through the Internet is treated as an independent unit of data without any relation to any other unit of data. (The reason the packets do get put in the right order is because of TCP, the connection-oriented protocol that keeps track of the packet sequence in a message.) In the Open Systems Interconnection (OSI) communication model, IP is in Layer 3, the Networking Layer. The most widely used version of IP today is IP version 4 (IPv4). However, IP version 6 (IPv6) is also beginning to be supported. IPv6 provides for much longer addresses and therefore for the possibility of many more Internet users. IPv6 includes the capabilities of IPv4 and any server that can support IPv6 packets can also support IPv4 packets.

IP
See “Internet Protocol”

IP Address
A four-byte number uniquely defining each host on the Internet, usually written in dotted-decimal notation with periods separating the bytes (for example, 134.177.244.57). Ranges of addresses are assigned by Internic, an organization formed for this purpose.

ISP
Internet service provider.

L

LAN
See "Local Area Network"

Local Area Network
A communications network serving users within a limited area, such as one floor of a building. A LAN typically connects multiple personal computers and shared network devices such as storage and printers. Although many technologies exist to implement a LAN, Ethernet is the most common for connecting personal computers and is limited to a distance of 1,500 feet. LANs can be connected together, but if modems and telephones connect two or more LANs, the larger network constitutes what is called a WAN or Wide Area Network.

M

MAC
(1) Medium Access Control. In LANs, the sublayer of the data link control layer that supports medium-dependent functions and uses the services of the physical layer to provide services to the logical link control (LLC) sublayer. The MAC sublayer includes the method of determining when a device has access to the transmission medium. (2) Message Authentication Code. In computer security, a value that is a part of a message or accompanies a message and is used to determine that the contents, origin, author, or other attributes of all or part of the message are as they appear to be. (*IBM Glossary of Computing Terms*)

MAC address
The Media Access Control address is a unique 48-bit hardware address assigned to every network interface card. Usually written in the form 01:23:45:67:89:ab.

Maximum Receive Unit
The size in bytes of the largest packet that can be sent or received.

Maximum Transmit Unit
The size in bytes of the largest packet that can be sent or received.

Mbps
Megabits per second.

MDI/MDIX
In cable wiring, the concept of transmit and receive are from the perspective of the PC, which is wired as a Media Dependant Interface (MDI). In MDI wiring, a PC transmits on pins 1 and 2. At the hub, switch, router, or access point, the perspective is reversed, and the hub receives on pins 1 and 2. This wiring is referred to as Media Dependant Interface - Crossover (MDI-X).

MTU
The size in bytes of the largest packet that can be sent or received.

P

packet
A block of information sent over a network. A packet typically contains a source and destination network address, some protocol and length information, a block of data, and a checksum.

Point-to-Point Protocol
PPP. A protocol allowing a computer using TCP/IP to connect directly to the Internet.

PPP
A protocol allowing a computer using TCP/IP to connect directly to the Internet.

PPPoA
PPPoA. PPP over ATM is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

PPPoE
PPPoE. PPP over Ethernet is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

PPP over ATM
PPPoA. PPP over ATM is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

PPP over Ethernet
PPPoE. PPP over Ethernet is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.

PPTP
Point-to-Point Tunneling Protocol. A method for establishing a virtual private network (VPN) by embedding Microsoft's network protocol into Internet packets.

Protocol
A set of rules for communication between devices on a network.

PSTN
Public Switched Telephone Network.

Q

QoS
See "Quality of Service"

Quality of Service
QoS is a networking term that specifies a guaranteed level of throughput. Throughput is the amount of data transferred from one device to another or processed in a specified amount of time - typically, throughputs are measured in bytes per second (Bps).

R

RADIUS
Short for Remote Authentication Dial-In User Service, RADIUS is an authentication system. Using RADIUS, you must enter your user name and password before gaining access to a network. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access. Though not an official standard, the RADIUS specification is maintained by a working group of the IETF.

RFC
Request For Comment. Refers to documents published by the Internet Engineering Task Force (IETF) proposing standard protocols and procedures for the Internet. RFCs can be found at *www.ietf.org*.

router
A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.

S

Segment
A section of a LAN that is connected to the rest of the network using a switch, bridge, or repeater.

Subnet Mask
Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router.

T

TCP/IP
The main internetworking protocols used in the Internet. The Internet Protocol (IP) used in conjunction with the Transfer Control Protocol (TCP) form TCP/IP.

U

Universal Plug and Play
UPnP. A networking architecture that provides compatibility among networking technology. UPnP compliant routers provide broadband users at home and small businesses with a seamless way to participate in online games, videoconferencing and other peer-to-peer services.

UTP
Unshielded twisted pair is the cable used by 10BASE-T and 100BASE-Tx Ethernet networks.

W

WAN
See “Wide Area Network”

Web
Also known as World-Wide Web (WWW) or W3. An Internet client-server system to distribute information, based upon the hypertext transfer protocol (HTTP).

WEB Proxy Server

A Web proxy server is a specialized HTTP server that allows clients access to the Internet from behind a firewall. The proxy server listens for requests from clients within the firewall and forwards these requests to remote Internet servers outside the firewall. The proxy server reads responses from the external servers and then sends them to internal client clients.

Wide Area Network

A WAN is a computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs).

Windows Internet Naming Service

WINS. Windows Internet Naming Service is a server process for resolving Windows-based computer names to IP addresses.

If a remote network contains a WINS server, your Windows PCs can gather information from that WINS server about its local hosts. This allows your PCs to browse that remote network using the Windows Network Neighborhood feature.

WINS

WINS. Windows Internet Naming Service is a server process for resolving Windows-based computer names to IP addresses.